THE DHS INFRASTRUCTURE PROTECTION DIVISION; PUBLIC-PRIVATE PARTNERSHIPS TO SECURE CRITICAL INFRASTRUCTURES

HEARING

BEFORE THE

SUBCOMMITTEE ON INFRASTRUCTURE AND BORDER SECURITY, AND SUBCOMMITTEE ON CYBERSECURITY, SCIENCE AND RESEARCH AND DEVELOPMENT

OF THE

SELECT COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

APRIL 21, 2004

Serial No. 108–45

Printed for the use of the Select Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE
23–278 PDF WASHINGTON : 2005

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

SELECT COMMITTEE ON HOMELAND SECURITY

Christopher Cox, California, Chairman

Jennifer Dunn, Washington
C.W. Bill Young, Florida
Don Young, Alaska
F. James Sensenbrenner, Jr., Wisconsin
W.J. (Billy) Tauzin, Louisiana
David Dreier, California
Duncan Hunter, California
Harold Rogers, Kentucky
Sherwood Boehlert, New York
Lamar S. Smith, Texas
Curt Weldon, Pennsylvania
Christopher Shays, Connecticut
Porter J. Goss, Florida
Dave Camp, Michigan
Lincoln Diaz-Balart, Florida
Bob Goodlatte, Virginia
Ernest J. Istook, Jr., Oklahoma
Peter T. King, New York
John Linder, Georgia
John B. Shadegg, Arizona
Mark E. Souder, Indiana
Mac Thornberry, Texas
Jim Gibbons, Nevada
Kay Granger, Texas
Pete Sessions, Texas
John E. Sweeney, New York

Jim Turner, Texas, Ranking Member
Bennie G. Thompson, MississPpi
Loretta Sanchez, California
Edward J. Markey, Massachusetts
Norman D. Dicks, Washington
Barney Frank, Massachusetts
Jane Harman, California
Benjamin L. Cardin, Maryland
Louise McIntosh Slaughter, New York
Peter A. DeFazio, Oregon
Nita M. Lowey, New York
Robert E. Andrews, New Jersey
Eleanor Holmes Norton, District of Columbia
Zoe Lofgren, California
Karen McCarthy, Missouri
Sheila Jackson-Lee, Texas
Bill Pascrell, Jr., North Carolina
Donna M. Christensen, U.S. Virgin Islands
Bob Etheridge, North Carolina
Ken Lucas, Kentucky
James R. Langevin, Rhode Island
Kendrick B. Meek, Florida
Ben Chandler, Kentucky

John Gannon, *Chief of Staff*
Stephen DeVine, *Deputy Staff Director and General Counsel*
ThomasDilenge, *Chief Counsel and Policy Director*
David H. Schanzer, *Democrat Staff Director*
Mark T. Magee, Democrat *Deputy Staff Director*
Michael S. Twinchek, *Chief Clerk*

Subcommittee on Infrastructure and Border Security

Dave Camp, Michigan, Chairman

Kay Granger, Texas, Vice Chairwoman
Jennifer Dunn, Washington
Don Young, Alaska
Duncan Hunter, California
Lamar Smith, Texas
Lincoln Diaz-Balart, Florida
Robert W. Goodlatte, Virginia
Ernest Istook, Oklahoma
John Shadegg, Arizona
Mark Souder, Indiana
John Sweeney, New York
Christopher Cox, California, ex officio

Loretta Sanchez, California
Edward J. Markey, Massachusetts
Norman D. Dicks, Washington
Barney Frank, Massachusetts
Benjamin L. Cardin, Maryland
Louise McIntosh Slaughter, New York
Peter A. DeFazio, Oregon
Sheila Jackson-Lee, Texas
Bill Pascrell, Jr., New Jersey
Kendrick B. Meek, Florida
Jim Turner, Texas, ex officio

Subcommittee on Cybersecurity, Science, and Research & Development

Mac Thornberry, Texas, Chairman

Pete Sessions, Texas, Vice Chairman
Sherwood Boehlert, New York
Lamar Smith, Texas
Curt Weldon, Pennsylvania
Dave Camp, Michigan
Robert W. Goodlatte, Virginia
Peter King, New York
John Linder, Georgia
Mark Souder, Indiana
Jim Gibbons, Nevada
Kay Granger, Texas
Christopher Cox, California, ex officio

Zoe Lofgren, California
Loretta Sanchez, California
Robert E. Andrews, New Jersey
Sheila Jackson-Lee, Texas
Donna M. Christensen, U.S. Virgin Islands
Bob Etheridge, North Carolina
Ken Lucas, Kentucky
James R. Langevin, Rhode Island
Kendrick B. Meek, Florida
Ben Chandler, Kentucky
Jim Turner, Texas, ex officio

CONTENTS

Page

STATEMENTS

WITNESSES

PANEL I

PANEL II

THE DHS INFRASTRUCTURE PROTECTION DIVISION; PUBLIC–PRIVATE PARTNERSHIPS TO SECURE CRITICAL INFRASTRUCTURES

Wednesday, April 21, 2004

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEES ON INFRASTRUCTURE
AND BORDER SECURITY,
AND
SUBCOMMITTEE ON CYBERSECURITY, SCIENCE AND
RESEARCH AND DEVELOPMENT,
SELECT COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The subcommittees met, pursuant to call, at 10:34 a.m., in Room 2212, Rayburn House Office Building, Hon. Mac THornberry chairman of the Cybersecurity subcommittee] presiding.

Present: Representatives Thornberry, Camp, Cox, Lofgren, Sanchez, Dicks, Cardin, Jackson–Lee, Christensen, Etheridge, Lucas, Chandler and Turner.

Mr. THORNBERRY. [Presiding.] This hearing will come to order. I appreciate the witnesses and the members who are here. There are obviously several substantial hearings going on at the same time. I know our witnesses will understand as people come and go. As you know, this is a joint hearing between the Subcommittee on Cybersecurity, Science and Research and Development, and the Subcommittee on Infrastructure and Border Security. Chairman Camp and I will be sharing the gavel.

Since we have two panels and two subcommittees today, I ask unanimous consent that all members submit opening statements for the record so that we can move ahead. Without objection, it is so ordered. I would also request our witnesses to work with us on that. I think we are going to have votes come at about 12:30 or 1:00. If you could work with us on summarizing your statements, then I would appreciate it. Without objection your full written statements will be made a part of the record.

PREPARED STATEMENT OF THE HONORABLE CHRISTOPHER COX, A REPRESENTATIVE IN CONGRESS, FROM THE STATE OF CALIFORNIA, AND CHAIRMAN, SELECT COMMITTEE ON HOMELAND SECURITY

Thank you Chairman Camp and Chairman Thornberry for holding this important hearing. I join you in welcoming our witnesses today, who will help us explore the Department's relationship with various critical infrastructure sectors.

I want to take this opportunity to commend Secretary Ridge, Under Secretary Libutti, Assistant Secretary Liscouski, and the men and women of the Information Analysis and Infrastructure Protection (IAIP) Directorate for their dedication and accomplishments in this critical area. They have had to build this Directorate from scratch, while facing both enormous expectations in a time of heightened alert and unrelenting scrutiny. IAIP gets a lot of attention because it is truly the nerve center of the great, new Department. IAIP is at the heart of the Department's core mission to prevent terrorism and protect the infrastructure that is vital to the security and economic well-being of our Nation.

The Homeland Security Act of 2002 requires IAIP to integrate information from various public and private sources to form a comprehensive picture of the terrorist threats we face, and to map this assessment against the vulnerabilities of our critical infrastructure to produce a prioritized and risk-based plan for securing our homeland. This is not a one-time task, but a continuous responsibility, in a dynamic and constantly changing environment. We have no choice but to continue to press IAIP to build the analytic capabilities necessary to carry out its mandate under the Homeland Security Act. Risk-based assessments produced by IAIP must guide both the Department's overall homeland security strategy and the allocation of resources to priority areas.

The President has exerted strong leadership in the effort to secure our critical infrastructure. He has issued a national strategy, as well as a Homeland Security Presidential Directive (HSPD–7). To secure our critical infrastructure both documents envision a strong, sustained public-private partnership. Eighty-five percent of our critical infrastructure is owned by the private sector, and it is appropriate that the private sector take a lead role in protecting these assets, with assistance—including the provision of actionable threat-based information—and oversight by the Federal government.

The President's fiscal year 2005 budget request includes $51.6 million for IAIP's "outreach and partnership" program, a 27-percent increase over the previous year. This increase is a strong indication of his commitment to enhancing the public-private partnership to protect critical infrastructure. Among other things, this program is intended to develop and coordinate strategic relationships between public and private entities for national planning, outreach and awareness, information sharing, and protective actions.

One key manifestation of the public-private partnership envisioned by the Homeland Security Act is the continued operation of—and in some cases, the creation of new—Information Sharing and Analysis Centers (ISAC) for critical infrastructure sectors. Part of this hearing will focus on obtaining information from the General Accounting Office on its soon-to-be-completed review of the ISAC model, and exploring how this model can be enhanced.

As we continue to work with DHS to enhance the public-private partnership, we must resist efforts to make DHS the regulator of more and more sectors of our economy. The Homeland Security Act clearly bars any such role for DHS, and we should alter that formula only with great caution. I see no reason to do so now or for the foreseeable future.

Mr. Chairmen, we share the bold vision of a safer America laid out in the Homeland Security Act, the national strategies, and HSPD–7. We are prepared to provide rigorous constructive oversight of critical infrastructure protection activities and to act as full partners with the Department, other government entities, and the private sector in helping realize that vision.

Thank you, Mr. Chairmen, and I yield back the balance of my time.

PREPARED OPENING STATEMENT OF THE HONORABLE SHEILA JACKSON-LEE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. Chairman, Thank you for convening this hearing on a subject that is extraordinarily important to the safety of the American public. I would like to welcome Assistant Secretary Liscouski back, as well as this distinguished panel. It seems that indeed the Department of Homeland Security is making progress in this area—putting people and facilities in place to protect our nation's critical infrastructure.

However, a chain is only as strong as its weakest link. For example, say I have a dozen chemical plants in my District in Houston. If we spend billions of dollars and five years and make 11 of them absolutely invulnerable, but we leave just one looking like the ones we all saw on *60 minutes* last fall, with unlocked gates, absent guards, and unprotected tanks of deadly gas—what have we accomplished? A would-be terrorist wanting to attack Houston would just have to spend an extra day plotting his attack—going through the phone book and driving by each chemical plant listed. It is essential that that we plug ALL of the holes. We need to know where our vulnerabilities are, and develop a comprehensive system to address those vulnerabilities.

That is why many of us have been standing behind the Ranking Member of this Committee, urging the DHS to complete a thorough risk assessment of our nation's critical infrastructure. That is why we need to have clear performance metrics for critical infrastructure protection. That is why we need seamless communication between federal and state governments and the private sector. To get those things done, we will need a fully staffed and functioning Office of Infrastructure Protection. Until then, we are all at risk.

Today we should hear the progress being made within DHS and in their work in the field. Do they have the funds, the expertise, and the authority they need to get the job done? Is those in the private sector willing partners? It will also be important to hear whether stakeholders outside the DHS are getting the guidance they need.

I look forward to the discussion, and to working together we these two subcommittees to ensure that we keep pushing the process forward.

So with that, let me turn directly to our witnesses. On our first panel, we have two distinguished witnesses. The first is Mr. Robert Liscouski, the Assistant Secretary for Infrastructure Protection from the Department of Homeland Security. He has been with us a number of times before. Secretary Liscouski, thank you for being here. You are recognized for a summary of your opening statement.

STATEMENT OF THE HONORABLE ROBERT LISCOUSKI, ASSISTANT SECRETARY, INFRASTRUCTURE PROTECTION, DEPARTMENT OF HOMELAND SECURITY

Mr. LISCOUSKI. Mr. Chairman, thank you for the opportunity this morning. It is always a pleasure to appear before your committees. I thank you again for your recognition of the importance of this topic. I do have an oral statement, but I will try to go through this as quickly as I can in recognition of our time constraints.

Since the inception of DHS, we have been working very strongly to develop partnerships with the private sector. We have made significant progress in evaluating and securing our greatest vulnerabilities. In order for this public and private partnership effort to succeed, we recognize that we have to increase our efforts at information sharing. To this end, we are making very good progress. Some would call it exceptional progress in expanding our information-sharing capabilities with respect to all types of information that must be shared, including vulnerability information, exploits, threats, incidents and best practices, as well as early warnings.

Our critical infrastructure sectors are very diverse, as you well know. Consequently, the level of collaboration and coordination with the Federal Government and each other within the context of the private sector varies widely between the sectors. We recognize these differences, and IAIP has developed a very facilitative process to work in partnership with the Federal sector-specific agencies as defined in HSPD–7, and to help sectors organize themselves as inclusively as possible to identify or construct the sector leadership entity for critical infrastructure protection.

At the operational level, IAIP works daily on a periodic and situational basis with ISACs, sharing information on threats and developing suggested protective measures and alerts and warnings. As you know, there are currently 14 ISACs spanning most of the HSPD–7 critical infrastructures. The ISACs serve as our gateway between DHS and the industry for tooling information sharing and provide the industry with information as an information clearinghouse for each sector.

Through up-to-date distribution lists maintained by the ISACs, DHS is able to quickly disseminate threat warnings to identify entities within each sector. To a lesser degree, however, ISACs and their members provide DHS with incident and suspicious activity. This has become very much more of a robust information-sharing capability. This information holds for us the potential for completing the situational awareness picture, together with the intelligence community and law enforcement, which is vital for us to understand the threats that we are facing.

My organization is responsible for maintaining and enhancing those relationships with the private sector through the ISACs and through other efforts. Our staff actively participates in ISAC-related advisory groups, committees, task forces and working groups to maintain day-to-day contact with those ISACs.

In protecting our country, we need to address the protection from a holistic perspective, not one which is artificially divided between a physical and a cyber-world. On January 28 of this year, the Department of Homeland Security, through the US–CERT, unveiled our national cyber security alert system, which is an operational system to develop and deliver targeted, timely and actionable information to Americans to secure their computer systems. We strive to make sure that the information provided is both understandable to all computer users, technical and non-technical alike, and reflects the broad usage of the Internet in today's society.

Our national strategy for cyber-security acknowledged one of the most important constituencies is the private sector. It is estimated that 85 percent of our critical infrastructure is, of course, owned and operated by the private sector, and the technology developed by the technology industry continues to fuel the growth and the evolution of the Internet, as well as obviously being ridiculously embedded in our business processes. In December 2003, the National Cyber Security Division co-hosted our first national cyber security summit, which allowed the Department to work side by side with leaders from industry to address key cyber-security issues facing the nation.

Other partnership efforts with the private sector include our National Cyber Security Alliance and Stay Safe Online, which is a public-private organization created to educate home users and small businesses on cyber security best practices.

Let me just take a moment to talk about the ISACs. The ISACs have emerged over the last several years as the primary conduit for critical information sharing between the Federal government and our infrastructures and key resources throughout the industries. The ISACs continue to evolve, although they began with a focus on cyber back in the PDD–63 days. They now include physical vulnerabilities as well. This emphasis has really been gaining momentum since September 11. This just demonstrates the recognition that the ISACs have matured, as well as our strategy to include our physical and cyber strategies are interlinked.

The blackout of August 14 last year is a good example of the cooperation and effective communication between IAIP and the industry, and specifically the electric power industry through the electric industries electric sector ISAC. At the time of the power outage, the electric sector ISAC had been well established and the lines of communication between the ISAC and IAIP were in place. Shortly after the blackout, the IAIP electric sector specialists were on the phone with the ES ISAC to establish a preliminary estimate of the extent of the outage to determine how far it had spread and to what extent.Following the discussions with the ISAC, we were able to make an assessment that the outage did not appear to have been caused by terrorist activity, and this information was quickly passed on to the Secretary and to the White House.

Every couple of hours throughout the night and somewhat less frequently over the next few days, the ES ISAC conducted conference calls with the industry representatives to assess restoration efforts, the results of which were daily summarized in situation reports that were provided to senior officials within DHS and the White House.

Since the creation of DHS, we have been leveraging newly integrated capabilities in the Department to reach out to the private sector. For example, in coordination with the U.S. Secret Service, shortly after the creation of DHS a financial services ISAC exercise was held in New York. The event was well received by the financial sector participants. We built on that effort and we are working with state homeland security advisers to continually put out more tabletop exercises. DHS has recently conducted exercises in Chicago, San Francisco and Houston, and we are currently conducting one in St. Petersburg, Florida with the FS ISAC.

The Administration and Congress have provided additional tools to enhance our information-sharing capabilities with the ISAC. I will just go through that very quickly. As the primary operational interface with the nation's critical infrastructures, my Infrastructure Coordination Division, or ICD, continues to pass timely and substantive threat information to the private sector. We regularly hold daily, sometimes weekly teleconferences. Sector analysts provide critical infrastructures and ISACs with threat updates on terrorist activities potentially affecting their systems and facilities.

In addition, the ICD sector analysts routinely assist our intelligence analysts from IA in preparing the warnings that identify and communicate infrastructure-specific threats and trends. The Critical Infrastructure Information Act was recently enacted at the request of the private sector, and provided implementing regulations to private industry with assurances that critical infrastructure information they voluntarily share with the government will be protected from release to the public from use in civil litigation.

The PCII program enables the Department to receive critical information that would not have been previously available to the government, thereby allowing a better understanding of threats and vulnerabilities and the security of our nation's critical infrastructure.

We recognize the need for better coordination for information flow in the private sector and we have established consequently the National Infrastructure Coordination Center under the Infrastructure Coordination Division. Now in its third month of official operation, the NICC provides operational awareness of the nation's critical infrastructures and key resources in collaboration with both private partners and our counterpart government agencies.

Another key component of our strategy is connectivity. With the announcement of the Homeland Security Information Network, HSIN, DHS provides a new capability for enhancing many of the critical infrastructures ISACs' capabilities to communicate with their sectors. The system provides a secure encrypted backbone capability for participants to communicate sensitive, but unclassified information with DHS, with each other, and other communities of interest which may have information useful to them. It provides a collaborative feature that allows government and industry participants to work together in real time on problem solving. It has an alerting and notification feature to disseminate information to members of a sector or across sectors.

The system provides a capability for sectors to interact with each other as necessity dictates. The features within that system provides for basic and common communication service among ISACs. I would be happy to discuss that further.

Let me just conclude by saying that in today's threat environment where threats and vulnerabilities are continuously evolving in both physical and cyber space, we need critical infrastructure sectors' coordination and cooperation and expertise and creativity to find the most effective, sustainable, consistent and measurable ways to protect their sectors. The partnerships we have developed and will continue to develop will improve upon the relationships we have, but they are absolutely key to the success of our goal to protect our nation and its critical infrastructure.

Mr. Chairman, thank you.

[The statement of Mr. Liscouski follows:]

Prepared Statement of the Honorable Robert Liscouski

Good morning, Chairman Thornberry, Chairman Camp, and distinguished members of the subcommittees. I am pleased to appear before you again today to discuss Information Sharing between the Department of Homeland Security and Critical Infrastructure Sectors.

The recent bombings in Madrid confirm that terrorists are willing to exploit a wide range of infrastructure vulnerabilities. That is why we must continue to be vigilant and flexible in our approach to infrastructure protection. We in the Information Analysis and Infrastructure Protection Directorate (IAIP) take that mandate to heart in our collective efforts and activities to protect the Nation.

Since the inception of DHS in 2003, working in a continuing partnership with private industry, we have made significant progress in evaluating and securing our greatest vulnerabilities. In order for this public-private partnership effort to succeed, increased information sharing is essential. To this end, we are making exceptional progress in expanding our information sharing capabilities with respect to all of the types of information that must be shared including vulnerability information, exploits, threats, incidents, best practices, and early warnings.

Today I will discuss with you an overview of the current level of relationships and information sharing we have with private industry, illustrating accomplishments with specific examples. Then I will describe recent initiatives we have implemented to enhance those relationships. Finally, I will discuss some new initiatives we are planning for later this year.

DHS and Private Sector Relationships

Any effective relationship with private industry requires engagement at all levels. IAIP works hard to maintain a comprehensive relationship with private industry, specifically focusing on the critical infrastructure sectors and the owners and operators of key assets. This relationship operates on three levels: (1) policy and strategy; (2) planning and implementation; and (3) operational execution.

Policy and Strategy

IAIP serves as the executive agent for two Presidential advisory committees: The National Infrastructure Advisory Council (NIAC) and the National Security Telecommunications Advisory Committee (NSTAC). Both bodies provide policy and strategic advice to the President on enhancing public-private partnerships and on specific strategic issues related to critical infrastructure protection.

The NSTAC is chartered to provide industry-based advice and expertise through the Secretary of Homeland Security to the President on issues and problems related to implementing national security and emergency preparedness (NS/EP) telecommunications policy. It is composed of up to 30 industry chief executives representing the major communications and network service providers and information technology, finance, and aerospace companies. Since its inception, the NSTAC has addressed a wide range of policy and technical issues regarding telecommunications, information systems, information assurance, critical infrastructure protection, and other NS/EP communications concerns.

The NIAC, through the Secretary of Homeland Security, provides the President with expert advice on the security of information systems for critical infrastructure supporting other sectors of the economy: banking and finance, transportation, energy, manufacturing, and emergency government services. Because information and physical security are inextricably linked within many critical infrastructure sectors, the Council has addressed issues that cover both. The NIAC is charged to enhance the partnership of the public and private sectors, propose and develop ways to encourage private industry to perform periodic risk assessments, foster improved cooperation among the Information Sharing and Analysis Centers (ISACs), DHS, and other Federal Government entities; and advise sector specific agencies with critical infrastructure responsibilities, sector coordinators, DHS, and the ISACs. The Council includes chief executives from industry, academia and State and local government.

Both the NSTAC and the NIAC work closely with the Administration and IAIP to identify key policy issues of importance to critical infrastructure protection.

Planning and Implementation

At the planning and implementation level, IAIP works with cross-sector bodies, such as the Partnership for Critical Infrastructure Security (PCIS). The PCIS Board consists of all the sector leadership entities that comprise the “sector coordination mechanism[s]” referred to in Homeland Security Presidential Directive 7 (HSPD–7). These leadership entities have been previously affirmed by the sector specific agencies. Private industry established the PCIS as a forum to partner across sectors and with the Federal Government to address critical infrastructure.

IAIP also works with the ISAC Council, whose members represent many of the ISACs established in infrastructure sectors. Private industry, on its own volition, organized this forum to share common issues and best practices, and to find common solutions. ISACs are established voluntarily by industry sectors to share information and analysis for alerts, warnings and advisories, and act as a communication vehicle for best practices and other security information tailored for each sector.

As a point of entry into the sector, sector leadership entities have the mission of facilitating sector strategy and policy as well as coordinating a wide range of critical infrastructure planning activities, that include national planning involving critical infrastructures, outreach and awareness, sector vulnerability assessments, requirements for sector information sharing, identifying sector-wide best practices, acting as the sector’s point of contact with the Federal Government at infrastructure protection meetings, and serving as the strategic communication point back into the sector and to its members from the Federal Government.

The critical infrastructure sectors are very diverse in their composition, culture, and operations. Consequently, their level of collaboration and coordination with the Federal Government, and with each other, varies widely between sectors. Recognizing these differences, IAIP has developed a facilitative process to work in partnership with the Federal sector-specific agencies (as defined in HSPD–7) to help the sectors organize themselves as inclusively as possible to identify or construct the “sector leadership entity” for critical infrastructure protection. This leadership entity could be an individual, entity or group. Examples of how IAIP actively engages in this sector development activity can be found today in the Agriculture and Food sectors (in partnership with HHS and USDA), the Public Health sector (in cooperation with HHS), the Postal and Shipping sector, the Water sector (in cooperation with EPA), and the Emergency Services sector.

IAIP leadership met frequently with both the PCIS and the ISAC Council throughout the last year, and continues to meet with them, to understand and gain deeper knowledge of sector issues from the private sector representatives on various aspects of infrastructure protection. Out of one of the briefings provided by IAIP to the ISAC Council, the Council, on its own initiative, developed a series of white papers on information sharing for its own use in strategic planning, and shared them with IAIP.

With the support of IAIP, the PCIS Board and the ISAC Council began holding joint meetings in December, 2003. They have worked jointly and independently on various initiatives. In joint sessions, DHS has provided comprehensive briefings on its initiatives and critical issues, which have led the joint PCIS/ISAC Council to begin identifying specific activities, tools/methodologies development, and programs undertaken by each specific sector and then shared across sectors as best practices to improve each sector's security. This study has helped each sector identify gaps as they compare their activities. This joint body represents a major forum for joint communication with the critical infrastructure sectors.

IAIP has embarked upon national level planning efforts that will involve the private sector in the development and/or implementation of the plan. Under HSPD–7, IAIP has embarked upon the development of the National Infrastructure Protection Plan (NIPP). This National Plan will cover the 13 critical infrastructure sectors and four categories of Key Resources. Sector-Specific Agencies both internal to and external to DHS will have the lead for drafting these 17 sector-specific plans, which will be integrated into the National Plan. The public-private partnership in this Plan will be realized through engaging the private sector in the planning process as represented by their ISACs, sector coordinators, and other recognized sector stakeholders so that their knowledge and information will be reflected in the substance of the Plan itself.

In a second national planning effort under HSPD-5, DHS's Office of Headquarters Integration Staff, along with the Department's directorates, is developing the National Response Plan. For the first time, the National Response Plan, which integrates the various federal response plans, will include the private sector as an essential element in preparedness, response, and recovery.

Relationships must be maintained at this level in order to assure coordinated and integrated plans and programs that utilize resources optimally and to assure engagement of operational leadership within the private industry for mutual planning and goals setting.

Operational Execution

At the operational level, IAIP works on daily, periodic and situational basis with ISACs sharing information on threats, developing suggested protective actions, and alert and warnings. There are currently 14 ISACs spanning most of the HSPD–7 critical infrastructures. ISACs serve as a gateway between DHS and the industry for two-way information sharing and provide the industry with an information clearinghouse for each sector. Through the up-to-date distribution lists maintained by the ISACs, DHS is able to quickly disseminate threat warnings to identified entities within each sector.

To a lesser degree, ISACs and their members provide DHS with incident and suspicious activity information. This type of information holds the potential for completing the situational awareness picture (together with Intelligence Community and Law Enforcement information) concerning possible threats to the nation's critical infrastructures. In my organization, the Infrastructure Coordination Division (ICD) and National Communications System (NCS) are the two IAIP divisions responsible for maintaining and enhancing relationships with the private sector through their ISACs, the latter with specific responsibility for the telecommunications sector. Staff from both divisions participate actively in ISAC related Advisory Groups, Committees, Task Forces and Working Groups and maintain day-to-day contact with the ISACs.

In addition, the Protective Security Division (PSD), also within the Office of Infrastructure Protection, has worked with owners and operators of specific categories of critical assets to develop and tailor protective practices for these assets. An example of this type of product is the guidelines for protecting refineries that the oil industry published last year. This type of work complements the "buffer zone" approach for communities that the division has developed and deployed over the last fourteen months. In addition, PSD is deploying regional/ field security representatives to work directly with the owners and operators of critical infrastructure facilities and community leaders to address protective measures. Together, these practices constitute a holistic approach to infrastructure protection, looking at the activity from a "whole systems" perspective, and providing for a "layered" defense for the nation's critical assets.

In support of integrated operations, DHS's predecessor agencies have granted security clearances to industry representatives when the purpose is to help the Federal Government maintain and enhance our national security, which includes critical infrastructure protection. Clearances historically have been given to individuals who have unique expertise, not available in government, on critical infrastructure protection, operations, or technology or who must take specific protective actions in response to classified information. In the past, IAIP sector analysts have specifically relied on ISAC and industry experts, generally with secret-level clearances, to help them assess sector threat, risk, and vulnerability information. In particular, these industry representatives work closely with DHS analysts to ensure that government-generated warning products (e.g. Advisories and Information Bulletins), when declassified to permit broad industry distribution, still contain information that provides "value added" actionable intelligence when disseminated to sector members. DHS is continuing to refine and working to accelerate the process for granting security clearances to key sector individuals to assist DHS, and ultimately their own sectors, regarding the production and receipt of timely and actionable threat information.

In February, 2003, President Bush issued the National Strategy to Secure Cyberspace ("the Strategy"). DHS recognized that in order to meet many of the mandates in the Strategy and other objectives addressing greater national cyber security, we needed to create an operational mechanism for building a cyber security readiness and response system. As such, through an initial partnership with the CERT Coordination Center (CERT/CC) at Carnegie Mellon University, we created the U.S. Computer Emergency Readiness Team, or US–CERT. Through that partnership, US–CERT is able to leverage, rather than duplicate, existing capabilities and accelerate national cyber security efforts. US–CERT provides a national coordination center that links public and private response capabilities to facilitate information sharing across all infrastructure sectors and to help protect and maintain the continuity of our Nation's cyber infrastructure. The overarching approach to this task is to facilitate and implement systemic global and domestic coordination of deterrence from, preparation for, defense against, response to, and recovery from, cyber incidents and attacks across the United States, as well as the cyber consequences of physical attacks. To this end, US–CERT is building a cyber watch and warning capability, launching the US–CERT Partnership Program to build situational awareness and cooperation, and coordinating with U.S. Government agencies and the private sector to deter, prevent, respond to and recover from cyber—and physical—attacks. Through its Internet portal, US–CERT is a crucial component of—and a distribution tool for—our cyber security awareness activities.

On January 28, 2004, the Department of Homeland Security through US–CERT unveiled the National Cyber Alert System, an operational system developed to deliver targeted, timely and actionable information to Americans to secure their computer systems. As the U.S. Government, we have a responsibility to alert the public of imminent threats and to provide protective measures when we can, or least provide the information necessary for the public to protect their systems. Furthermore, it is also important to inform the public about the true nature of a given incident, what the facts are, and what steps they can and should take to address the problem. The offerings of the National Cyber Alert System provide that kind of information, we have already issued several alerts and the initial products in a periodic series of "best practices" and "how-to" guidance messages. We strive to make sure the information provided is understandable to all computer users, technical and non-technical, and reflects the broad usage of the Internet in today's society. As we increase our outreach, the National Cyber Alert System is looking at other partners to distribute information to as many Americans as possible.

As the strategy acknowledged, one of our most important constituencies is the private sector. It is estimated that eighty-five percent of America's critical infrastructure is owned and operated by private companies, and technology developed by industry continues to fuel the growth and evolution of the Internet. In December 2003, the National Cyber Security Division (NCSD) co-hosted the first National Cyber Security Summit in Santa Clara, California with the Information Technology Association of America, TechNet, the Business Software Alliance, and the U.S. Chamber of Commerce. This event was designed to energize the public and private sectors to implement the Strategy. The Summit allowed the Department of Homeland Security to work side-by-side with leaders from industry to address the key cyber security issues facing the Nation. Five interest areas were established to focus specifically in the areas of:

- Increasing awareness
- Cyber security early warning
- Best practices for information security corporate governance
- Technical standards and common criteria
- Security across the software development lifecycle

Perhaps most importantly, the Summit served as a call to action. It represented a logical transition point from developing a national strategy to energizing the public-private partnership to implement concrete, measurable actions to improve the security of America's cyber systems. Over the past few weeks, summit participants have put forward options for potential solutions in each of these key areas for both the public and private sector. We are excited that the private sector is showing such initiative and we are committed to working together.

DHS is also a sponsor of the National Cyber Security Alliance (NCSA) and *StaySafeOnline,* a public-private organization created to educate home users and small businesses on cyber security best practices. Other NCSA sponsors include: The Federal Trade Commission, AT&T, America Online, Computer Associates, ITAA, Network Associates, and Symantec. DHS is providing matching funds to expand the NCSA end-user outreach campaign, which will include a Fall 2004 Public Service Campaign to increase awareness among Americans about key cyber security issues.

In operational relationships of this kind, adding value, efficiency and customer orientation is the key to building trust and sustaining relationships. IAIP has worked hard to enhance its capabilities in this regard over the last year with these activities. These relationships represent on-going efforts that are essential for efficient planning and implementation coordination. The long term commitment of communications between the federal government and the private entities is an essential element of building successful public-private partnerships.

Private Public Partnerships Information Sharing

Adequate, actionable information is an essential enabler for all facets of critical infrastructure protection, from deterrence to response. Congress recognized its importance in the new tools it provided to DHS to obtain and protect, analyze and disseminate information from a wide variety of sources. Private industry owners and operators of critical infrastructure have long understood their responsibility for assuring their operations under a multitude of circumstances ranging from accidents to natural disasters. They now must add terrorism to the list of natural and man-made hazards they must consider and accommodate in their investments and response preparedness. The Federal government alone cannot protect this nation's expansive and widely distributed national infrastructures. IAIP needs private industry to be fully engaged in our national CIP program. Consequently, two-way information sharing with the owners and operators of critical infrastructures remains one of our highest priority public private partnerships.

Current Information Sharing Initiatives

The Information Sharing and Analysis Center (ISAC) has emerged over the last several years as a primary conduit for information sharing between the Federal government and many critical infrastructures and key resource industries. Each ISAC structure and operations tends to reflect the culture, structure and operating processes of their sector. The ISACs continue to evolve. They began with a focus on cyber security vulnerabilities and incidents. Since September 11, 2001, most share information on physical incidents as well.

ISACs have widely varying levels of maturity and capability. ISACs have served a valuable role in private partnership information sharing. The purpose of the ISAC is to provide an efficient conduit for dissemination, sharing and communications of indications, warnings, and advisories related to potential threats vulnerabilities and incident data.

The Northeast Blackout of last year is a good example of cooperation and effective communications between IAIP and the Electric Power industry through the industry's Electric Sector—ISAC. At the time of the power outage the ES–ISAC had already been well established and lines of communication between the ISAC and IAIP were in place. By approximately 4:30 p.m. EDT, 15 minutes after the initiation of the power outage, the IAIP's electric sector specialist was on the phone with the ES–ISAC to establish a preliminary estimate of the extent of the outage and to determine whether it had ceased to spread. Following discussions with the ISAC, we were able to make an assessment that the outage did not appear to have been caused by terrorist activity. This information was immediately elevated to Secretary Ridge and to the White House.

Every couple of hours throughout the night, and somewhat less frequently over the next several days, the ES–ISAC conducted conference calls with industry representatives to assess restoration efforts. These calls were summarized in a Situation Report that was provided to senior officials within DHS and to each IAIP Infrastructure Sector lead for cross-infrastructure sharing purposes (since every sector depends upon electricity). In addition, the ES–ISAC structure was used effectively to share information with other industry sectors that are dependent on electricity. For example, on the evening of the power outage, the IAIP electric power staff addressed a conference call of the Financial Sector-ISAC and was able (based on earlier ES–ISAC inputs) to estimate the duration of the interruption of power supplies to New York City. In summary, the August 14th power outage demonstrated that the ISACs are an effective mechanism for receiving information from the private sector as well as for providing information to the private sector during a crisis.

A long standing example of the utility of ISACs is the National Communications Center Telecommunications-ISAC, which is the primary DHS interface with the Private Sector for the telecommunications infrastructure. Built on an existing information sharing body, the NCC Telecom-ISAC is grounded by well-established trust. This mature, close relationship with industry is Government-supported, which facilitates the ISAC's ability to provide a value-added service, reaching out to the entire sector. This has provided a great role model for other ISACs.

In the past, the Federal Government would conduct readiness and terrorism exercise in the absence of private sector participation. For example, in the TOPOFF-1 and TOPOFF-2 exercise series, the private sector owners and operators of infrastructure were excluded from "exercise play", with the sole exception of hospitals, which were always one of the key operations being ″stressed and tested″ in those types of exercises. In contrast, based on prior planning and coordination by the U.S. Secret Service component of DHS, a Financial Services (FS)–ISAC Table Top Exercise was held in New York, March 2003 soon after the standup of the Department. DHS staff attended the exercise to observe the scenario play and to ensure that participants were aware of DHS's role, including ICD role, in aiding with real-world recovery operations. The event was well received by the financial sector participants.

Building on this effort and working with the state homeland security advisors, DHS has continued these exercises in, Chicago, San Francisco, Houston, and now, concurrent with this testimony, from 19–22 April 2004, the FS–ISAC is hosting its next Tabletop exercise in St. Petersburg, Florida. The exercise will include two days of interactive tabletop play. DHS is sponsoring this event and staff will be actively participating in the exercises.

From the lessons learned of TOPOFF-2 and these other table top exercises, IAIP recognizes the need to engage our private sector partners in these planning and execution of these national level exercises. Exercises, of all kinds, tabletop, command post and full scale; are powerful 'best practice' training tools and provide another venue for information sharing. IAIP plans to continue to include the private sector in future exercises whenever it makes sense to do so.

New Information Sharing Initiatives

The Administration and Congress have provided additional tools to enhance information sharing with the private sector. I will now discuss IAIP's new information sharing initiatives.

As the primary operational interface with the nation's critical infrastructures, ICD continues to pass timely and substantive threat information to the private sector. At daily and/or weekly teleconferences, sector analysts provide the critical infrastructures via the ISACs with unclassified threat updates on terrorist activities potentially affecting their systems and facilities. In addition, classified threat briefings are presented to cleared ISAC representatives and their industry members on a quarterly or semi-annual basis. To maintain appropriate situational awareness for each sector—a key division objective—ICD analysts on an *ad hoc* basis also provide timely assessments of high threshold threats to critical infrastructures through the ISACs. In addition, ICD sector analysts routinely assist IA analysts in preparing warning products that identify and communicate infrastructure-specific threats and incident trends.

The National Infrastructure Coordinating Center (NICC) uses the Infrastructure Protection (IP) Executive Notification Service (ENS) to quickly notify ISAC leadership and Sector Coordinators of critical infrastructure events ranging from notification of imminent threats, dissemination of sector-specific warning products, and changes in national threat level. ENS delivers rapid internal and external messaging capability among government and private sector partners and provides Interactive Secure Authentication, which ensures confidentiality of communications, as well as confirmation of receipt.

Protected Critical Infrastructure Information

Critical to the Department of Homeland Security's mission is the ability to effectively share information with homeland security partners across the country to better protect the nation's critical infrastructure. The Critical Infrastructure Information (CII) Act and implementing regulations provide private industry assurances that critical infrastructure information they voluntarily share with the government will be protected from release to the public and from use in civil litigation. The PCII Program enables the Department to receive critical infrastructure information that would not have previously been available to the government, thereby allowing for a better understanding of threats, vulnerabilities and the security of the nation's critical infrastructure.

With the protection from FOIA disclosure offered by the CII Act, the private sector can share sensitive and confidential information that can be analyzed to identify threats and vulnerabilities. Such analysis will provide the basis not only for developing measures to deter the threats and mitigate the vulnerabilities to which the critical infrastructure is exposed, but also for improving Federal, State, and local governments' emergency preparedness posture to respond to any attacks more effectively.

The benefits to private industry are both practical and patriotic. Information sharing will result in better identification of risks and vulnerabilities, which individual companies can use to help protect their assets. By voluntarily sharing such critical information, private industry demonstrates responsiveness to Government need and the public good. Private industry is demonstrating good corporate citizenship that may save lives and protect our hometowns. By participating in the PCII Program, industry is helping to safeguard and prevent disruption to the American economy and way of life.

National Infrastructure Coordination Center (NICC)

The NICC is currently developing capabilities towards its targeted operational capacity. Now in its third month of official operation, the NICC is collecting and analyzing best practices. While this analysis begins with watch center models, it also includes management practices, information sharing systems, and other process development models from a broad range of industries. The NICC will also work with its IAIPs public and private sector partners to ensure that its operational models most effectively and efficiently meet their needs.

DHS designed the NICC specifically to maintain operational awareness of the nation's critical infrastructures and key resources in collaboration with both private partners and counterpart government agencies. The NICC also, by design, provides DHS with the ability to coordinate information sharing between government, ISACs, and other industry partners. The NICC functions as an extension of the Homeland Security Operations Center (HSOC).

Homeland Security Information Network

With the announcement by the Secretary of the Homeland Security Information Network (HSIN) in March, DHS provides a new capability for enhancing many of the critical infrastructure ISACs' capabilities to communicate with their sectors. The system provides a secure encrypted backbone capability for participants to communicate Sensitive But Unclassified (SBU) information with DHS, with each other, and other communities of interest that have information that may be useful to them. It provides a collaborative feature that allows government and industry participants to work together in real-time on problem solving. It has alerting and notification features to disseminate information to members of a sector or across sectors. The system provides the capability for sectors to interact with each other on the system as necessity dictates. These features provide support for a basic and common communications service among ISACs.

By providing access to these capabilities to the critical infrastructure ISACs, IAIP adds value as a partner to the ISACs by removing duplication of costs in implementation and operations, and accelerates the development of value of the ISACs to their sectors. From experience with its use through the JRIES community (consisting of law enforcement at Federal, state and local levels) the collaborative and real-time aspects of the system actually increases the pace and volume of information sharing. Pilots with volunteer critical infrastructure sectors will begin this year, with support from the Infrastructure Coordination Division.

We have seen great progress in two way information sharing with the private sector and these examples are illustrative of our efforts.

Conclusion

This Administration has upheld a consistent policy that public private partnerships be one of the pillars of national critical infrastructure protection. Partnerships are an essential element described in every national strategy document that we have published on homeland security and critical infrastructure protection. This policy recognizes the new environment of terrorism, where both threats and vulnerabilities are continuously evolving in both physical and cyber space, will require an unprecedented adaptability and cooperation of the stakeholders. Since 85 percent of the critical infrastructures are owned and operated by private industry, how could a sustained effort be institutionalized to protect them? Only a full understanding by the stakeholders of their own vested interests related to this issue could sustain such an effort and commitment. Public-private partnerships are the only means that is responsive enough and adaptive enough to accomplish our national goals in a scalable, sustainable, and effective way.

We have learned many lessons about developing effective partnerships both from our legacy agencies and from our own experiences since DHS was implemented in 2003. I would like to share three of these with you today. Lesson 1—Partnerships require a set of mutually determined objectives and deliverables to achieve a value proposition and trust. Lesson 2—Participation in planning and objectives setting is essential to the success of the partnership. Both sides must understand the expectations, values, concerns, risks and individual objectives of each participant. Lesson 3—Constant communication between all of the parties is an essential imperative.

With years of experience by agencies that are now part of DHS, the successful partnerships built between federal lead agencies and their counterparts in industry were those where the federal lead agencies educated and learned, convened, listened and responded and then supported their industry counterparts who took the lead to implement programs to protect themselves. The Federal government sharing useful, actionable information on threats induces greater information sharing by industry in return. Making it easy for industry to receive and provide information, providing products and services in return, based on that information, and working with owners and operators to develop and implement consistent and generally accepted protection practices, will add value to any partnership.

In all relationships, there are challenges. Strong long-term relationships depend, however, on how well the participants handle, learn from, and adapt to those challenges. Some lessons learned from the recent past in our dialogue with industry include involving them in planning, mutual goals setting and development of operational learning, such as input into our national plans, the NIPP and NRP, and direct participation in major exercises such as TOPOFF3. We have responded and adapted to many of the needs and expectations of industry in support of their protection strategies and programs.

Some private institutions have committed tremendous resources in time and money to supporting this national initiative, not just for their individual institution but for their industry as whole. Even before 9/11, some were doing so. Terrorists have innumerable weapons and targets of choice in our open society. In order to sustain an effective national CIP program, we need critical infrastructure sectors' cooperation, expertise and creativity to find the most effective and efficient ways to protect their sectors. It is incumbent upon DHS to develop and strengthen these partnerships and we will do so because there is more to do to help secure our homeland.

Mr. THORNBERRY. Thank you.

Also on our first panel, we have Mr. George Newstrom, who is the Secretary of Technology and Chief Information Officer for the Commonwealth of Virginia. He also serves as the Chairman of the Security Committee of the National Association of State Chief Information Officers. Secretary Newstrom, thank you for being with us, and you are recognized for 5 minutes to summarize your statement.

STATEMENT OF THE HONORABLE GEORGE NEWSTROM, SECRETARY OF TECHNOLOGY, COMMONWEALTH OF VIRGINIA

Mr. NEWSTROM. Thank you, Mr. Chairman and members of the committee. I will summarize my statement. You have the full text in front of you right now. The Chairman has already introduced me and the two hats that I come to you with today.

At NASCIO, I serve as the Chair of the Security Committee. This committee addresses the role of information and communications technology, both in terms of how it supports the wider needs of state homeland security directors and how state governments should be protecting their critical information assets. We also oversee NASCIO's Interstate Information Sharing and Analysis Center, the ISAC, which arose from a 2002 memorandum of understanding with DHS's Infrastructure Coordination Division led by Jim Caverly.

Information infrastructure is only part of America's critical infrastructure that is under attack everywhere all the time. Unfortunately, cyber attacks on a national scale are still treated as secondary to any physical threat, whether it is chemical, biological, radiological, nuclear or explosive. NASCIO believes that while cyber terrorism per se is still an emerging threat, we must press forward toward a coordinated intergovernmental approach to protecting government's critical information assets if we are to ensure that critical government business functions, especially those supporting homeland security, will be available when needed.

If we can secure our systems from hackers and organized crime, we will have gone a long way toward securing them from terrorist and enemy nation-states. NASCIO has long realized the interdependence of Federal, state and local information systems which drive the need for intergovernmental approach. Toward that end, we produced a document in 2002 titled Public Sector Information Security, a call to action for public sector CIOs that emerged from a forum convened by NASCIO in the wake of 9–11. We also convened a roundtable discussion that included local, state and Federal participants here last July.

The primary lessons we have learned are that government ICT, information and communications technology personnel, should be considered core competencies to state and local emergency response capabilities because without them, everything from databases to wireless communications first responders cannot do their job. Also, given the fact that states, counties and cities are the primary mechanism for the delivery of critical services to citizens, including Federal programs, if the information systems of states or local governments go down, the ability of the other levels of government to do business within jurisdictions will be significantly impaired, if not interrupted. This creates a cascading effect.

While the CIO is charged with protecting the state's critical information assets, he or she is also charged with managing the day-to-day operations of a wide variety of information systems and infrastructures that support first responders in homeland security leadership. Up to now, homeland security has primarily been defined as those systems involving law enforcement and emergency managers. However, as state efforts fuse information from intelligence and all-hazard incident management purposes become more sophisticated, a wide range of information systems will be drawn together in an effort from public safety, public health, transportation and agriculture, among them.

Homeland security at the state and local level is less about organizational change and more about cultural adjustment. Homeland security, like technology, requires an enterprise approach that synchronizes and harmonizes disparate parts under a common umbrella. Key to this success with this cultural change is achieving vertical and horizontal sharing and integration of information, something that requires effective application of technology. This will require the CIO, with statewide oversight, to help manage the development and deployment of systems that can meet the ever-changing needs of homeland security decision makers.

As a caution and an urge to the Federal Government, we ask that the Federal Government consolidate its information-disseminating capability. While it may be necessary to separate public safety, military and cyber efforts, we should not have multiple, uncoordinated information dissemination efforts within each of these categories as we do now. Virginia knows from first-hand experience that the FBI and DHS are issuing separate information products to law enforcement and non-law enforcement communities respectively. This makes it difficult for state homeland security directors and CIOs to understand the full spectrum of threats faced by states, without staying abreast of multiple channels and fusing the information internally.

NASCIO knows by the work with other states that the other Federal agencies, particularly those in the Departments of Justice and Health and Human Services, are issuing cyber alerts to state and local programmatic counterparts which are not incorporated in the National Cyber Security Division, NCSD, of DHS. NASCIO would be willing to work with Mr. Amit Yoran and the Federal Chief Security Officers Council to develop an intergovernmental warning process so state CIOs, homeland security directors and program-specific leadership receives coordinated, consistent and timely alerts and notices.

As the 9–11 commission has heard now on many occasions, the issue may be less on what and how much information we know, but how knows it and who they share it with. In the area of cyber security, we are doing well at countering attacks on infrastructure after they happen. Isn't our real objective to try to identify potential attacks in advance so that we can avert costly efforts to eradicate them once they happen? The only way to do this is by connecting the dots, sharing information across Federal and state agencies in a timely and focused manner.

NASCIO has been actively engaged in sharing cyber threat and incident information with and among states as part of our interstate ISAC program. We have also gathered information and targeted requests from DHS and provided feedback on the effectiveness of various information sharing analysis practices. We have drawn on the goodwill of our corporate partners to provide the states with supplemental information to help them respond to fast-moving threats like worms and viruses.

Regarding specific efforts by the Commonwealth of Virginia, as members of today's committee know very well, Virginia is home to the Pentagon, one of the three sites in the United States that were attacked on September 11. The memory of that day and its aftermath continue to permeate the consciousness of those serving in Virginia State government and the local community, while serving as a guide for Virginia's efforts in homeland security and critical information protection. To respond to this challenge, Virginia has three specific efforts under way. One is the Secure Virginia Panel. The second is the National Capital Critical Infrastructure Vulnerability Assessment Project. Three is the Virginia Alliance for Securing, Computing and Networking. You have all those in the detailed comments in my testimony.

The first one is a public-private partnership that the Governor of Virginia established within 30 days of coming into office. The second one is the District of Columbia, the State of Maryland and the Commonwealth of Virginia working together to ensure the entire region's assets. The third is the Virginia Alliance for Securing Computing and Networking is in the educational community to secure our research networks that are very instrumental to all of us.

Mr. Chairman and members of the subcommittee, Virginia and all the states represented by NASCIO are moving forward in the context of protecting critical infrastructure from physical and cyber vulnerabilities. This effort is requiring new ways of thinking and new types of relationships between Federal and state entities. Much progress has been made, but there is much to be done.

I enjoy a close working relationship with Virginia's homeland security team, state as well as local, as well as the leaders of the Federal efforts in DHS. I know that we do not have all the answers. We may not even have all the questions. But we know that protecting our critical assets from cyber and physical threat is a key to ensuring the safety of Americans and protecting our economic security.

My message to you, in conclusion, is first, despite the continuing daily attacks on our nation's information infrastructure, cyber security is still seen as a secondary threat and the interdependence of Federal, state and local systems absolutely requires closer and a more cohesive approach. second, we are encouraged by the organization and the leadership at DHS to move smartly and timely with the assistance of their state and local partners, and particularly the recent evaluation of the ISAC approach and the new opportunities for effective change that it represents.

NASCIO will do what it can to assist by working with DHS, ICD and NCSD divisions to arrive at the most effective approach, and also by developing the states and local addendum to our national security strategy.

Let me take a moment and thank Robert Liscouski, Assistant Secretary, sitting next to me, as well as Jim Caverly, who heads ICD, and Amit Yoran, the Director of the National Cyber Security Division, as well as Steve Cooper, the CIO of the Department of Homeland Security. These folks have worked with us, as well as George Foresman, Virginia's Assistant to the Governor for Commonwealth Preparedness, to meet the goals that we have outlined.

Mr. Chairman, thank you, and members of this committee for the opportunity to be here with you today.

[The statement of Mr. Newstrom follows:]

Prepared Statement of the Honorable George C. Newstrom

Chairman Thornberry, Chairman Camp and Members of the Subcommittees,

Thank you for inviting me to appear before you today. I am before you today wearing two different hats: one representing the Commonwealth of Virginia as its Secretary of Technology and the second as the Chair of the Security Committee of the National Association of State Chief Information Officers (NASCIO).

I would like to offer my perspective on the issues of partnership and information sharing with particular regard to Virginia's cross-sector efforts to secure its critical and information infrastructures and NASCIO's efforts to coordinate DHS's interaction with the states on these matters. Virginia and NASCIO appreciate your attention to this important matter and willingness to get input from a state and organization that have direct stakes in the outcome. We believe that success in cross-sector infrastructure assurance and information sharing will be the result of persistent effort by many parties, advancing in spurts during times of urgency and more incrementally during times when trust and cooperation must be solidified for the long haul.

Efforts By NASCIO

At NASCIO, as I indicated, I serve as chair of their Security Committee. This committee addresses the role of state Information and Communications Technology (ICT) both in terms of how it supports the wider needs of state homeland security directors and in how state governments should be protecting their critical information assets. We also oversee NASCIO's Interstate Information Sharing and Analysis Center (ISAC) efforts, which arise out of a July 2002 memorandum of understanding with DHS's Infrastructure Coordination Division (ICD), led by James Caverly.

Protecting Governments' Critical Information Assets

The information infrastructure is the only part of America's critical infrastructures that are under attack everywhere, all the time. Unfortunately, "cyber" threat on a national scale is still treated as secondary to any physical threat whether it be chemical, biological, radiological, nuclear, and explosive. NASCIO believes that, while cyber-terrorism *per se* is still an emerging threat, we must press forward toward a coordinated, intergovernmental approach to protecting governments' critical information assets if we are to ensure that critical governmental business functions—especially those supporting homeland security—will be available when needed. If we can secure our systems from hackers and organized criminals, we will have gone a long way toward securing them from terrorist and enemy nation states.

NASCIO has long realized the interdependencies of federal, state, and local information systems, which drives the need for an intergovernmental approach. Toward that end, we produced a document in 2002, titled "Public-Sector Information Security: A Call to Action for Public-Sector CIOs" that emerged from a forum convened by NASCIO in the wake of 9/11. We also convened a roundtable discussion that included local, state, and federal participants last July here in Washington.

The primary lessons we have learned are that government ICT personnel should be considered a core component to state and local emergency response capabilities, because without everything from databases to wireless communications the first responders cannot do their jobs. Also, given the fact that the states, counties, and cities, are the primary mechanisms for delivering critical services to citizens—including federal programs, if the information systems of a state or local government go down, the ability of the other levels of government to do business within that jurisdiction will be significantly impaired, if not interrupted. This creates a cascading effect.

Supporting State Homeland Security Decision-Makers

While the CIO is charged with protecting the state's critical information assets, he or she is also charged with managing the day-to-day operations of a wide variety of information systems and infrastructure that support first responders and homeland security leadership. Up to now, homeland security ICT has primarily been defined as those systems serving law enforcement and emergency managers. However, as state efforts to fuse information for intelligence and all-hazards incident-management purposes become more sophisticated, a wide range of information systems will be drawn into the effort, including those from public safety, public health, transportation, and agriculture among others.

Homeland Security at the state and local level is less about organizational change and more about cultural adjustment. Homeland security, like technology, requires an enterprise approach that synchronizes and harmonizes disparate parts under a common umbrella. Key to succeeding with this cultural change is achieving vertical and horizontal sharing and integration of information—something that requires effective application of technology. This will require the CIO, with statewide oversight, to help manage the development and deployment of systems that can meet the ever-changing needs of homeland security decision makers while maintaining appropriate levels of privacy and security. Our adversaries will continue to change their tactics. Therefore, our information systems must be able to help state homeland security directors and DHS gather the information they will need to counter these evolving threats.

Focused Action By The Federal Government Is A Necessity

It is so important that the federal government consolidate its information dissemination capability. While it might be necessary to have separate public safety, military and cyber efforts, we should not have multiple, uncoordinated information dissemination efforts within each of those categories as we do now. Virginia knows from first hand experience that the FBI and DHS are issuing separate information products to the law enforcement and non-law enforcement communities respectively.

This makes it difficult for state homeland security directors and CIOs to understand the full spectrum of threats faced by the state without staying abreast of multiple channels and fusing the information internally.

NASCIO knows by way of its work with all the states, that other federal agencies, particularly those in the departments of Justice and Health and Human Services, are issuing cyber alerts to their state and local programmatic counterparts, which are not incorporated into the National Cyber Security Division (NCSD) of DHS alert products. NASCIO would be very willing to work with Mr. Yoran and the new Federal Chief Security Officers Council to develop an intergovernmental warning process so that state CIOs, homeland security directors, and program specific leadership receives coordinated, consistent as well as timely alerts and notices.

As the '911 Commission' has heard now on many occasions, the issue may be less on what and how much we know but who knows it and who they share the information with. In the area of cyber security, we are doing well at countering attacks on our infrastructure AFTER they happen. Isn't our real objective to try to identify potential attacks in advance so that we can avert the costly efforts to eradicate them after they happen? The only way to do this is to 'connect the dots'—share information across federal and state agencies in a timely AND focused manner.

Sharing Information with the States

NASCIO has been actively engaged in sharing cyber-threat and incident information with and among the states as part of our Interstate ISAC program. We have also gathered information for targeted requests from DHS and provided feedback on the effectiveness of various information sharing and analysis practices. We have drawn on the goodwill of our corporate partners to provide the states with supplemental information to help them respond to fast-moving threats like worms and viruses.

We applaud Amit Yoran's recent efforts at the National Cyber Security Division (NCSD) to engage the states directly and make the US-CERT a valuable tool for the entire ICT-using community, including individual U.S. citizens. We are currently working with Jim Caverly at ICD to further refine our ISAC program. We know that DHS, NASCIO, and individual states have very limited resources to contribute to any information sharing effort. Therefore, we seek to have an information sharing and analysis program that is as transparent as possible between DHS and the states. We also want it to provide targeted services with a definable return on the sweat equity investment by the states. This will take time. But, NASCIO has found its partners at NCSD and ICD to be very receptive to our suggestions for improvement and we remain committed to ensuring the success of any information sharing efforts with the states.

Our NASCIO Security Committee currently has two deliverables in progress for 2004, which might be of interest to you:

- A state and local addendum to the *National Strategy to Secure Cyberspace.* Following a meeting with DHS and White House cybersecurity leadership, the National Governors Association (NGA) began working with NASCIO to take on the joint role of serving as *ad hoc* coordinators for the state and local sector. In that role, we will be forming a task force or working group to produce a brief addendum that will highlight the key sector implications of the strategy. It will also provide an opportunity to put forth some additional recommendations for action by our sector. This group will include state, county, and municipal chief information officers (CIOs) and chief information security officers (CISOs) as well as participants from the telecommunications directors, utilities commissioners, and educational community.
- Defining the role of the CIO in homeland security decision support.NASCIO will shortly be releasing a detailed brief on the role of the CIO in supporting intra-state intelligence and situational awareness efforts, which combine to provide homeland security leadership with what we are calling "decision support." It will include several calls for very precise state and federal action that we hope will prepare the states to fulfill the goals of the recently released National Incident Management System (NIMS) as well as support the ongoing deployment of new and enhanced information sharing networks by DHS CIO, Steve Cooper.

Efforts Specific to the Commonwealth of Virginia

The efforts undertaken by the Commonwealth of Virginia in securing its critical physical and infrastructure has been primarily focused on the development of partnership among key state and local agencies, the private sector and Virginia's institutions of higher education to develop and implement strategies for securing and maintaining critical infrastructure.

As members of today's committees know very well, Virginia is home to the Pentagon one of the three sites in the United States that was attacked on September 11, 2001. The memory of that day and its aftermath continue to permeate the consciousness of those serving in Virginia's state government and local communities while serving as a guide for Virginia's efforts in homeland security and critical infrastructure protection component.

To respond to these challenges, the Commonwealth of Virginia has three specific efforts underway that will be discussed today. These efforts are:

- The Secure Virginia Panel
- National Capital Region—Critical Infrastructure Vulnerability Assessment Project
- The Virginia Alliance for Secure Computing and Networking (VA SCAN)

The Secure Virginia Panel

As one of his first acts of office to respond to the challenge of protecting the Commonwealth, the Governor of Virginia, Mark R. Warner, signed Executive Order 7 on January 31, 2002, establishing the Secure Virginia Initiative and convening the Secure Virginia Panel. In bringing together state government, local government and the private sector, the Secure Virginia Panel and its working groups has served as the primary conduit for developing public-private partnerships to deal with the challenges in preparing for emergencies and disasters of all kinds, including terrorism.

Through the Critical Infrastructure Working Group (CIWG) of the Secure Virginia Panel, Virginia is tackling many of the same challenges that are also being addressed by the federal government. Also comprised of members representing state government, local government and the private sector, the CIWG is specifically charged with making recommendations that strengthen cyber and physical security for critical infrastructure throughout the Commonwealth. By identifying failure and inter-dependency points in critical infrastructure security and developing a methodology for prioritization of those points, the CIWG is attempting to answer three critical questions:

1. What critical infrastructure is needed to keep government operational?
2. How does the Commonwealth of Virginia best coordinate with local government and the private sector?
3. What organizational structure is best suited to ensuring a coordinated approach to both cyber and physical security of critical infrastructure located in Virginia?

To answer these questions, the CIWG has outlined six objectives that it plans to meet by December 2004. These objectives are as follows:

1. Development of a governance model that can best coordinate critical infrastructure protection and risk mitigation.
2. Identification of critical infrastructure.
3. Identification of inter-dependency and failure points in critical infrastructure protection.
4. Development of a methodology to prioritize critical infrastructure protection initiatives.
5. Assignment of responsibility within state government for coordinating critical infrastructure cyber and physical security efforts.
6. Coordination among the public sector, private sector and institutions of higher education to ensure the development and utilization of a consistent assessment methodology.

These efforts are facilitated by prior recommendations that have been developed by the Secure Virginia Panel. Specifically, in 2002, the Panel recommended legislative changes that would protect from FOIA the disclosure of critical infrastructure information submitted to state government by the public sector. Titled the 'Sensitive Records Protection Act' (HB 2210), the legislation was passed by the 2003 General Assembly and subsequently signed into law by the Governor.

National Capital Region—Critical Infrastructure Vulnerability Assessment Project

The vulnerability of the National Capital Region was made painfully obvious on September 11th, 2001. The coordinated partnership by the federal government, the states of Virginia and Maryland and the District of Columbia to the unique situation of our Capital region demonstrates the cooperative approach towards homeland security and critical infrastructure protection that is being pursued today.

Under the auspices of the post 9 /11 funding provided by Congress, Urban Area Security Initiative Grant Program as well as the Department of Justice Community Oriented Policing (COPS) program, funded through the Department of Homeland Security's Office for Domestic Preparedness, a leading regional effort for critical infrastructure protection in the National Capital Region is being lead by George Mason University. This effort is part of a broader set of NCR initiatives being orchestrated by the Mayor of DC and Governor's of Virginia and Maryland under the auspices of their representatives on the Senior Policy Group in partnership with community leaders.

The Urban Area Security Initiative (UASI) is a program that helps develop sustainable models to enhance security and overall preparedness to prevent, respond to, and recover from acts of terrorism in high-density population centers. Specifically, UASI was created to "enhance the ability of first responders and public safety officials to secure the area's critical infrastructure and respond to potential acts of terrorism. Initially, seven metro areas were identified: New York City, Washington, D.C., Los Angeles, Seattle, Chicago, San Francisco, and Houston. For the 2004 fiscal year, this number increased to 50, now including smaller cities such as Orlando, Florida, and New Haven, Connecticut.

For the National Capital Region, a strategy was developed to provide a strategic direction for preventing and reducing vulnerability in the region. The strategy was developed based on a number of inputs: the results of an assessment completed by communities in the National Capital Region in July 2003, the National Strategy for Homeland Security, the Eight Commitments to Action for the National Capital Region, and the State Template published by the Homeland Security Council. The Strategy focuses on four areas: planning, training, exercise, and equipment. George Mason's activities fall within the planning area.

The grant from the Department of Justice Community Oriented Policing (COPS) program, complementing the efforts undertaken through the UASI initiative, focuses on the telecommunications, water, energy, and transportation sectors in the Commonwealth of Virginia.

In cooperation with five universities, including James Madison University, the University of Virginia, Virginia Polytechnic Institute and State University (Virginia Tech), the University of Maryland, and Howard University, the NCR Critical Infrastructure Vulnerability Assessment Project focuses on improving regional and sectoral methodologies for conducting vulnerability assessments. The ultimate objective of the project is to raise the level of security in the National Capital Region by ensuring that critical infrastructure sectors address the most important security concerns. The project seeks to enhance the capability and capacity of the National Capital Region to reduce vulnerability, minimize damage and increase resiliency. In addition to the regional universities engaged in this initiative, GMU is also working collaboratively with industry and government.

The Virginia Alliance for Secure Computing and Networking (VA SCAN)

The Virginia Alliance for Secure Computing and Networking (VA SCAN) is a partnership of universities that seeks to strengthen information security programs within the Commonwealth of Virginia. The partnership includes security professionals from George Mason University, James Madison University, the University of Virginia (UVA), and Virginia Polytechnic Institute (VA Tech) as well as researches and staff from the Institute for Infrastructure and Information Assurance (3IA) at JMU, the Center for Security Information Systems at GMU, and the joint GMU/ JMU Critical Infrastructure Protection Project (CIPP). Representatives from other Virginia institutions, including Mary Washington College, Radford University, The Virginia Institute of Marine Science, The College of William and Mary, Virginia Commonwealth University, and the Virginia Military Institute serve as advisors to VASCAN partners.

VA SCAN began offering products and services in March of 2003. The offerings are based on the principle that the most lasting improvements to security programs can be made not by performing security functions for organizations, but rather by educating and guiding management and staff teams in defining and carrying out their own security strategies and operations. Some of the products and services offered include:

- A Virginia—Critical Infrastructure Response Team (CIRT) group for tracking security threats
- Self-assessment checklist for Commonwealth of Virginia security standards
- Security policy development and security awareness training
- Onsite training and security instructional materials
- Onsite consulting on a variety of security topics and an "ask the expert" email service
- Web-based toolkit of security tools and best practices

Concluding Remarks

Mr. Chairman and members of the subcommittees, Virginia and all the states represented by NASCIO are moving forward in the context of protecting critical infrastructures from physical and cyber vulnerabilities. This effort is requiring new ways of thinking and new types of relationships between public federal and state efforts.

Much progress has been made but there is much more to do. I enjoy a close working relationship with Virginia's homeland security team, state as well as local, as well as the leaders of the federal efforts at DHS. I know that we do not have all of the answers and we frankly do not have all of the questions. But we know that protecting our critical assets from cyber and physical threats is key to ensuring the safety of Americans and protecting our economic security.

In conclusion, my message to you is that, despite the continuing, daily attacks on our nations information infrastructure, cybersecurity is still seen as a secondary threat, and the interdependence of federal, state and local systems absolutely require a closer, more cohesive approach. Secondly, we are encouraged by the organization and leadership at DHS to move smartly and timely with the assistance of their state and local partners, and in particular, the recent re-evaluation of the ISAC approach and the new opportunities for effective change that represents. NASCIO will do what it can to assist by working with DHS's ICD and NCSD divisions to arrive at the most effective approach, and also by developing the state and local addendum to our National Strategy.

Let me take a moment to thank Robert Liscouski, Assistant Secretary for Infrastructure Protection, DHS; Jim Caverly, director, Infrastructure Coordination Division; Amit Yoran, director, National Cyber Security Division; Steve Cooper, chief information officer, DHS and George Foresman, Virginia's Assistant to the Governor for Commonwealth Preparedness for all that they do towards our common goals.

Mr. Chairmen, I thank you and the members of your committees for the opportunity to testify before you today.

Mr. THORNBERRY. Thank you. Some very good points.

I yield to Chairman Camp.

Mr. CAMP. Thank you, Mr. Chairman.

I appreciate both of your testimonies here this morning. Assistant Secretary Liscouski, obviously we are very interested in the role of the ISACs or the Information Sharing and Analysis Centers in being a link to the private sector in terms of infrastructure protection. I wonder to what extent you feel that they have fulfilled their expectations. Do you still view them as the primary public-private partnership link? To that extent, I know that under your authority there is a significant budget for public outreach, nearly $50 million. It is my understanding none of that has gone to the ISACs. I think a little bit of funding might help them in their role.

So I am really interested in to what extent you consider their role important, and still that key link.

Mr. LISCOUSKI. Mr. Chairman, thank you for the question, and to the point about the partnership with the ISACs. We view them as critical, along with the other sector-specific agencies and the sector coordinators, to ensuring that we have not just the good links to the private sector, but most importantly the information coming back into DHS to understand what their concerns are.

Let me just take a moment to address your question by just taking a step back for a second to say that we recognize that when PDD–63 was established, the direction the ISACs were going into was a very good direction, but there was very little leadership from the private sector to step up to really help guide those ISACs to provide to the government what their requirements were.

When we established DHS and I became responsible for those ISACs, and particularly based upon my private sector background, it was clear to me that the model we had to change had to be one which was much more of a private sector-led model, rather than a government-led model. To that end, and it is a philosophy we live by today, we established a capability within my organization for Infrastructure Protection, and specifically with the Infrastructure Coordination Division, to be that central point of contact for us into the ISACs; to establish the links, to formalize those links, but most importantly to develop or receive the requirements back from those ISACs.

Based upon that, we developed our fiscal year 2004 funding profile to ensure that the funding stream that went to the ISACs met their initial requirements and their evolving requirements. So we set aside $16 million for outreach that would be used to assist the ISACs in developing and forming themselves, as well as assisting them in their communications capabilities. To date, we have spent approximately $6.5 million to support the ISACs in the form of creating a common communications mechanism under the Homeland Security Information Network, which is a common platform for communications which we are rolling out to the ISACs, which effectively provides a no-cost entry for companies to form an ISAC and then gain access to this information, as well as other outreach efforts to include administrative support and research support vis--vis George Mason University's Critical Infrastructure Protection Project, which is something we also fund.

We have been working with the ISACs. Specifically back in December, we had an ISAC sector summit in which we solicited from the ISACs their very specific requirements for how they thought they needed to be funded and where their funding priorities are and where they remain.

Mr. CAMP. What do you think the principal challenges are in having the ISACs reach their fullest potential?

Mr. LISCOUSKI. It depends upon the ISAC. It is not a one-size-fits-all model. I think the expectation we have is that we really need their requirements to be well defined as it relates to both information sharing on the two-way street. I think we have overcome many of the big challenges, for instance the establishment of the ISAC Council, which as it relates to the ISAC is our point of entry into the broad ISAC community to make sure we get collective thought well represented back into the government so we understand what those needs are. That is one challenge we have overcome.

I think the other challenge is them defining specifically what their requirements are in terms of not just linking up with DHS, but most importantly conveying to us what their information-sharing requirements are.

Mr. CAMP. I think one of the critical things is the coordination of risk assessment by DHS. I think that is probably one of their most crucial roles. It appears as though there are multiple requirements for risk assessment depending on the agency, TSA or Coast Guard, or whatever. What steps are being taken to resolve this overlap and multiple levels or layers of risk assessment that really can be an undue burden on the private sector?

Mr. LISCOUSKI. I agree with that statement. As you know when DHS was formed, TSA had already been in existence and had been moving out in its effort very, very aggressively to try to connect up with the private sector; similarly with the Coast Guard going out and doing what they were doing; similarly with Secret Service and others.

So we immediately began to coordinate the efforts for critical infrastructure protection and come up with common vulnerability assessments and risk analysis and capabilities that could be spread across the entire spectrum. Over the past year, we have been working on that, but we have really been able to even more consistently address this through the implementation of the Homeland Security Presidential Directive Number Seven, which has really given us the impetus to bring together all the various Federal agencies, not just within DHS, but across the Federal Government, to understand these programs and what their priorities are and how each respective sector-specific agency is going to be addressing those priorities. That is a normalization effort that we are currently engaging in right now.

Mr. CAMP. OK, thank you. I see my time has expired.

Mr. LISCOUSKI. Thank you, sir.

Mr. CAMP. Thank you, Mr. Chairman.

Mr. THORNBERRY. Thank you.

The gentlelady from California, Ms. Lofgren.

Ms. LOFGREN. Thank you, Mr. Chairman.

Just a note, we have both Secretary Ridge and Secretary Powell downstairs in the Judiciary Committee, so even though I am very eager to hear what you have to say, I may be bopping down there in the near future.

I hate to be a nag, but I am going to complain again, Mr. Liscouski, about the lateness of your testimony. The committee rules require that testimony be submitted 48 hours in advance. Once again, yours was received last night at 7:04 p.m., as a matter of fact is when we go the email. It is just not sufficient time for the committee members to review the testimony. There is a reason for the rule and I think it is offensive for the whole committee. I hope that that is the last time that this occurs. It is just not acceptable to me. I hope that that will not occur again.

I want to ask a broad question, if I may. We need a comprehensive risk assessment of our nation's critical infrastructure. It seems to me that that has not yet been completed. I would like to know when the comprehensive critical infrastructure risk assessment will be completed. Specifically, I would like to know who within the IAIP is in charge of this risk assessment work. I would like to know the number of employees that are assigned to its production and the number of contractors and the number of detailees, the specific dollar amount that is assigned to produce this analysis.

I would like to note that I have a number of questions. We probably will not be able to get through with them. In the past, we have submitted questions to the Department and generally we never get answers to them from any of the witnesses, including yourself. So I would like a commitment for those questions that we cannot get through that we actually will get written responses from you. I will not hold you accountable for our friend Asa Hutchinson and the others who have not responded, but I hope that the answers can be prompt.

And if you could address the questions that I have asked now, I would be very appreciative.

Mr. LISCOUSKI. Yes, ma'am. I apologize again for the lateness of the submission of the testimony. With respect to the questions that you just referenced, I know I personally reviewed questions that you have submitted to me, so I know that they are a work in progress and we will check on what the status of those is so you can get them in a timely way.

With respect to the comprehensive risk assessment, as I have said prior when I have appeared before this committee and others, that is an ongoing process. If we do our job right, and I know this can be taken out of context, we will continuously revise that list. We have over 33,000 assets identified in our national asset database, for which we are doing analysis on those risk assessments and continually updating those things.

As you are aware based on my previous testimony, the interdependencies between all those assets continuously change based upon the threats. So we will never be satisfied based upon the evolving threat environment, that we should sit back and say that because we have done one risk assessment for one particular asset, that we should not go back and revisit that. So that is a continuous process.

I know it is a difficult thing, but the enormity and the complexity and the scope of our critical infrastructure protection mandates that we continuously revise and review our risk posture and the changing threats, both of group capabilities, as well as their intent. second, this is not just a DHS effort, but this is a Federal Government as well as a state and local and a private sector effort. So many of those things over which we have responsibility, we do not directly control and therefore our ability to get fidelity in the comprehensive listing of all the assets is dependent upon the cooperation we have with the various entities who play in that space.

Homeland Security Presidential Directive Number Seven gives us a significant leg up on our ability to coordinate these activities within the Federal sector. So it is not just DHS in the context of TSA and other responsibilities that Under Secretary Hutchinson may have, as well as my own group, but it is clearly those within DOT, Department of Agriculture, HHS, and others, which have similar types of responsibilities.

So this is a national problem, as you well know, and not just a Federal problem. So I would suggest to you that we are working extremely hard and we have made significant progress over the past year in really aggregating a list. That has given us a very clear understanding of the major priorities that we have to address and we are addressing those priorities.

Ms. LOFGREN. If I could, we do understand that we are not going to come up with a list and then never revisit it. Obviously, it is an ongoing process. Am I to understand from your testimony that the critical infrastructure risk assessment has been completed and now it is a matter of updating it? Or if not, what are the milestones?

Mr. LISCOUSKI. The milestones are the outreach program that we have with the state and local and Federal sectors. We have tasked them specifically to identify what they believe are critical, based upon the definition in the Patriot Act, which is what we always go back to, to ensure that we have clarity of what that list is. Oftentimes we find that what we have done to identify critical assets in the United States and what the states and local municipalities and cities have done often do not reconcile. So we spend a significant amount of time reconciling those assets, doing the consequence analysis and the impact of attack on the exploitation and vulnerabilities of those assets. So no, ma'am, it is not complete, but much of that is outside the control of DHS per se, but based upon the input that we get from folks in the respective jurisdictions that you all represent, as well as other Federal agencies.

Ms. LOFGREN. My time has expired, but I would ask that you respond to me. By the way, you did not give me the number of employees and detailees.

Mr. LISCOUSKI. I would be happy to get back to you in writing, if I may.

Ms. LOFGREN. If you could also provide a list of what you have prepared, the milestones that you have achieved, your timelines for the rest of it, and then to the extent that there are departments that you are dependent on that have not actually produced, list them and tell us what they have not produced so that we can then inquire with them. I think that is essential.

Mr. LISCOUSKI. I think it is. Let me just level-set the expectation here. We are asking questions for which are not quite sure what the answers are necessarily. I could ask each one of the Representatives for input on what they think is critical. There might be things in there that you know about, that I do not know about. So I am asking a question on which I am totally dependent upon the folks at the local level for the answers.

So to suggest that there is a finite number of assets over which I have some clarity in terms of a number, then I can measure a milestone that I am at the 80 percent level or the 90 percent level, to be quite candid with you, is a little unrealistic. We do not know all the assets out there.

Ms. LOFGREN. My time has expired, Mr. Chairman.

Mr. THORNBERRY. Thank you.

The gentlelady from California, Ms. Sanchez.

Ms. SANCHEZ. Thank you, Mr. Chairman.

Thank you once again for being before us. I know that we had an opportunity, Chairman Cox and Chairman Camp and myself, to sit down with you about two or three weeks ago to discuss this whole list of 1,700 critical sites. I did gain a lot of information, but we were the only ones, and I know some of it is secret information. But I think for the ability for some of the committee members here today, if you could share with us what intelligence or other information is used to determine the priorities by which you are putting these critical pieces of infrastructure on this list that you are working on.

Once the infrastructure is prioritized, what happens to it when it is on this list? I know that you and I talked about how you discuss this with local law enforcement, where this critical infrastructure might be, and that they then are supposed to approach in particular private businesses. Can you tell us how that is going? How do you follow up on whether anything gets done? Maybe some private business does not really respond to local law enforcement when they come forward and say you need to secure this particular area in a better way, and here might be some ways in which you could do that. Have you provided assistance to these local law enforcement agencies to help them get that job done, of implementing it on the ground?

Mr. LISCOUSKI. Thank you for your question. I always enjoy the opportunity of explaining this methodology. Just to underscore the complexity of this effort, in working with the private sector and our colleagues on the state and local level, we have developed a methodology which we are putting out as widely as we can in terms of best practices, of understanding what those risks are and how to assess those risks.

When we come up with a prioritized list, it is typically based upon a five-step process. The first step in that process is clearly identification of those assets, those things that need to be protected. Although that sounds like a very simple thing to do, it is who owns those things, and really what is the definition that we are putting around that infrastructure component, what are the interdependencies. There is a significant amount of analysis that goes on to the front end of this process to identify the asset.

Ms. SANCHEZ. And you are doing this? Or are you using the state and local people's input into these assets in trying to understand what they are?

Mr. LISCOUSKI. It is actually all of that. It is DHS. It is our state and local partners. It is the private sector. This is a highly interdependent process. The second step in that process is clearly understanding the vulnerabilities, what can be exploited. The third part of that process is understanding the consequence of the exploitation of that vulnerability. The consequence analysis is based upon a number of factors, not least of which is the consequence of loss of life or economic impact, or the threat to our national security.

That gives us a prioritization around then what do we need to be looking at first, independent of a threat environment, because there are many different continuums upon which we have to operate. But the baseline, the sort of steady-state continuum that we operate under is one which is an absence of threat. So we look at one from a vulnerability and consequence of loss perspective.

The fourth step in our process is understanding what programs we have to put out around to remediating or mitigating those vulnerabilities. The fifth step, which if you asked about challenges, is the most challenging. That is the metrics component, the output, the output of understanding not just what programs are being implemented to address those vulnerabilities, but are they actually being implemented. More importantly, are they being implemented well enough to address the vulnerabilities themselves.

Then we layer on top of that threat information. So as we get a better understanding of what vulnerabilities are, we then understand how groups can exploit those vulnerabilities based upon their capabilities and their intent, and our ability to understand from an intelligence perspective who is operating against us that might be targeting those vulnerabilities in a particular sector.

That is how we prioritize them. We are actively engaging in revising that prioritized list to make sure that we can understand from a threat perspective what we need to address first. That is done in concert with our counterparts, particularly in the Information Analysis Division of IAIP and other members of the community, and then clearly with the ability to understand what is going on at the state and local level from their priority perspective.

One part of your question also addressed what are we doing to help state and locals. That becomes a part of what their capabilities are. We find out, again, the rising tide, so to speak, of DHS does not float all the boats. We have to ensure that we can address some specific gaps with the state and locals, particularly at the local level, again working with the homeland security advisers in partnership in addressing those gaps. DHS may provide best practices. We may work with them on the ODP grant process, or we may go in there, depending on the specific sector and the specific vulnerability against the threat, to assist them in training and practical applications of technology to ensure that we can counter that threat.

Ms. SANCHEZ. I think my time is up, Mr. Chairman.

Mr. THORNBERRY. Does the gentlelady have a quick follow-up?

Ms. SANCHEZ. A really quick follow-up. In looking through your plans and your goals for this year, I just pulled out an example. You had in there a desire to send out your team to take a look at about 270 specific sites with relationship to chemical possibilities. Of those 270, you have so far this year visited 17, two of which are now non-active sites. Given that record, just how far along are you on this plan of identifying and actually taking a look and making back recommendations?

Mr. LISCOUSKI. Again, thank you the opportunity to address a misperception. The last number you just addressed, the 17 or the top-most identified critical sites that we saw around the United States from a chemical sector perspective, they were addressed in fiscal year 2003, actually. The ones that we thought we needed to have the greatest impact on very shortly, we did that very early on in the creation of DHS. The number actually of 360 sites we are addressing in fiscal year 2004 through our Buffer Zone Protection Plan. We have been very aggressively going out there and visiting sites, providing common vulnerability assessments.

Our assistance to these sites is one which is either a physical visit, coordinated with state and locals and our homeland security advisers, in which we will send DHS teams out to conduct an assessment if we believe it is necessary, or we will provide other types of assistance, such as common vulnerability assessments, best practice methodologies, interaction with them in a way that allows them to bolster their own security without us having to actually make a site visit, working with our state and local partners to do the site visits.

We do not have enough bandwidth within DHS, nor was the model ever envisioned that we would actually go out and do assessments for the entire industry. We are working with our industry partners, with our state and local authority partners, to ensure that they know how to do vulnerability assessments and report that information back to us. So we are making very good progress. I do not have the exact number. I will be happy to get back to you on that number. But the number for fiscal year 2004 is on track, and I am putting significant pressure on my team to make sure they stick with that number.

Ms. SANCHEZ. Thank you, Mr. Chairman.

Mr. THORNBERRY. Thank you.

Chairman Cox?

Mr. COX. Thank you.

I want to thank both of our witnesses for outstanding testimony. This is a very, very important aspect of what we are doing. In fact, I think it is fair to say that infrastructure protection, and IAIP is the heartbeat of this new Department. I want to thank you, the Assistant Secretary, Mr. Liscouski, and Mr. Newstrom for helping us focus on this today. Mr. Liscouski, you and Secretary Ridge, Under Secretary Libutti and all the men and women of IAIP deserve our congratulations and our thanks for what you are doing in this critical area.

You have had to build your capability from scratch. This is not one of the 22 agencies that were merged together to form this Department. You have had to face enormous expectations through periods of heightened alert and of course intense scrutiny from the Congress because there is nothing more topical or more urgent before the Congress. I think mostly you get all of this attention because IAIP is in fact the nerve center of this enormous new Department and you are the heart of the Department's core mission.

With 85 percent of what we are denoting as critical infrastructure key assets to preserve our way of life in the event of attack in the private sector, this kind of coordination that we are talking about today is just absolutely important. The ISACs are not creatures of either the Homeland Security Act or any other Federal statute. To a certain extent, there is some experimentation going on with this. ISACs are constructed along an industry model. They are stovepipes in that respect. They are not cross-jurisdictional. We have other councils that you are also sharing information with that are cross-jurisdictional.

I want to ask, as the first of my two questions, whether or not you think that we should continue this experimental practical R&D process, or whether it is time for us to formalize legislatively the ISAC process and fund it. The second question I have relates particularly to a portion of your testimony, Mr. Newstrom. You brought to our attention that you know by way of your work with all the states that other Federal agencies, particularly those in the Departments of Justice and HHS, are issuing cyber alerts to their state and local programmatic counterparts, that these are not incorporated into the national Cyber Security Division of DHS alert products. At the same time, there is not an intergovernmental warning process that focuses everything from one place in the Federal Government.

You bring to our attention that among others, the 9–11 Commission has emphasized that it is not just how much we know, but how knows it, that is really important. The vastness of the Federal Government, complemented by the vastness of all our state governments, and then the private sector on top of it and cross-jurisdictional concerns that we have makes this vitally important.

Mr. Liscouski, you have told us, and I have every reason to believe you, that DHS is now able to quickly disseminate threat warnings to identified entities within each sector. It seems to me that is a very significant accomplishment. The next step is to consolidate warnings issued by IAIP to a single node for dissemination to our private partners. The ultimate step would be to consolidate warnings issued across the Federal Government to a single node, which the Homeland Security Act contemplates. I want to ask you both also to address that.

If you could, I hope that you did not forget my first question. Talk first about whether the ISAC model is one still under development and whether we ought to consider other complements to it, or whether we are starting to get a feel for exactly what we want to do in this area.

Mr. LISCOUSKI. Thank you, Chairman Cox. I will give you my private sector perspective, if I could, to add some fidelity around my thinking. I think it is important to understand, as I said earlier, this is not a government model. This really needs to be a private sector model.

To your point about the formalization of the ISACs, I think they are clearly making some very, very good progress in developing a way that the industries can come together through the ISAC model. My philosophy that I am providing as guidance to the implementation of this and working with the ISACs and the private sector, is one which really puts the onus on them to define what their requirements are.

For a moment, I just want to digress to talk a little philosophically about how information flow goes within the industries, and how the information flow that goes through industries is oftentimes predicated upon what types of problems they solve. Because industries themselves, companies themselves have many diverse problems over which they have to share information as well. My personal background within aFortune 50 firm that I worked for, was that we often looked at not just problems of manufacturing processes and the threats that they might be subjected to. That might require us to go out to one information pool to figure out how we do that, but then the supply chain that feeds that manufacturing process might put us into a different information pool or a different community of interest. Similarly in the cyber world, that may also put us into another community of interest; similarly with the HR world.

We have to provide the capability for the private sector to align itself with information or communities of interest based upon their needs. We need to facilitate that process as best we can. My fear in terms of legislating the ISACs would be from the perspective of making it more rigid than the process really should allow. Information flow really needs to be as free-flowing, and we need to, from my perspective, facilitate information flow processes. If we put labels on what that process is at a top level based upon some sector alignment, I think that is appropriate. If we get too down to a granular level, we will create artificial stovepipes that will not facilitate the collaborative process between companies and between industries that is so necessary today.

Industries create this process irrespective of what the government involvement is. That is why industry associations are out there. That is why we do things at a level between security officers between companies at a very high level to ensure we have very informal networks for information. I think the important model here is one that represents a very highly integrated network model, meaning that if you notice terrorist groups today operate in a highly networked environment themselves. They leverage technology to be able to communicate and develop expertise in areas that they can share in a highly diverse networked way, which puts the information at the edges of their organization.

Similarly with information we need to be sharing here in the private sector, facilitated by the government, needs to be equally diverse and robust in terms of its flow. It has to be highly networked, highly capable of changing as situations change. Frankly, I do not think the government can facilitate that in any way that would allow us to do anything but create a stovepipe if we get too involved in the process. I would be interested in Mr. Newstrom's comment about that.

I think the government's value-added in this process is relevant information. I think if we can provide information into the process that allows us to know with some degree of confidence that the private sector knows what they need to be doing and they are sharing information and solving the problems, we have ourselves a successful model.

I think we are going to wind up having to look at this very carefully. I think you are going to hear on the second panel today from Diane VanDe Hei how they are implementing their information-sharing analysis center in an extremely diverse sector. It is representative here. I think one thing we have to be careful of is, these sectors are extremely diverse and we have to ensure that whatever we create today can survive not just in what we know about current diversity, but emerging diversity.

I do not know if that answered your question fully enough. I would be happy to add more, but I do not want to take any more from Mr. Newstrom's time, but I would be happy to address this more.

Mr. NEWSTROM. Thank you, Chairman Cox, for the question. I was hoping to get away without getting a question. Mr. Liscouski was doing such a great job in answering the others.

Let me talk about the second part of that question, which was how it work together; what kind of fragmented information we are getting right now. As I say that, I also commented about how it has gotten substantially better. In fact, it has gotten exponentially better in the last 12 months since the inception of DHS and the creation of ICD and NCSD. Prior to that, let me suggest the information flow was fragmented. It was not focused. Around cyber security, it almost did not exist or it was sporadic at best.

Now, with ICD, with NCSC, what Mr. Yoran is doing, what Jim Caverly is doing, it is programmatic. It is institutionalized. Even better, they have developed a partnership model with state officials, with local officials as well as the private sector. It is very apparent that that is the methodology, that is the direction that DHS is going. So we applaud that direction. We ask that we continue that direction.

Certainly, there is still some fragmentation that I addressed in a couple of my comments. I hope that over a period of time, hopefully of a short period of time, we can even address those. But I do want to comment that the communications in the last six to eight to twelve months has been substantially better than it was prior to that.

Does that answer the question, Chairman Cox?

Mr. COX. I think what Mr. Liscouski wants to know, let's go to that question.

Mr. LISCOUSKI. Let me just address how we are trying to better coordinate. Let me just qualify this as a preface by saying, I clearly understand that there were gaps in our information flow in the past. We did not know what the FBI was sending out. The FBI did not know what we were sending out when we first got started, as well as all the other agencies. We addressed that very quickly with the FBI. We have coordinated alerts going on. We still may send them out independent channels. The FBI has the responsibility of sending it out to the state and local law enforcement authorities, over which DHS does not have domain, and we with the private sector and our state and homeland security advisers.

We are reconciling the fact that the creation of the messages that go out now are coordinated and co-developed and cleared off on by both agencies. That is a step in the right direction. As Mr. Newstrom pointed out, we still have other agencies in the Federal Government that are sending out alerts, and we are reconciling that through the Homeland Security Presidential Directive Seven effort, which is really articulating some of the rules of the road, not just the lanes in the road, of how we need to communicate so we have a good message.

In the past, I was concerned that when messages went out, one message said black, the other one said white, to the same audience from two different senders, that would cause confusion. Now, we may have two different senders or multiple senders, but a much more consistent message says white from all the senders or black from all the senders, so we have consistency around the messaging.

To that end, and getting more consistency around that, let me just address a couple of different ways we are doing that. When it comes to a significant incident, particularly in the cyber arena, Mr. Yoran has created the Cyber Interagency Incident Management Group which stands up with not just the Federal partners, but state and local and the private sector to address incidents that have to be actively and dynamically managed. He chairs the Chief Information Security Officer Forum, or CISO Forum, which is an education and networking venue for government security executives. Again, it is not just alerts and warnings, but we are getting consistency around best practices through that forum, as well as the G–FIRST, the Government Forum of Incident Response and Security Teams, which is a 24/7 government-oriented group that does an analysis that accelerates and enhances an agency's ability to identify a cyber crisis.

So we have a number of forums, depending upon the particular audience, that gets more coordination and centralization of the problem-solving approach and the alert mechanisms that are going out there. We have work to do, but we are on the right path. I am confident that as we continue to move along this path, we will get more consistency, so that stakeholders like Mr. Newstrom and others will not have to worry about getting multiple messages from multiple providers.

Mr. COX. Thank you.

Mr. THORNBERRY. The Chair recognizes the Ranking Member of the full committee, Mr. Turner.

Mr. TURNER. Thank you, Mr. Chairman.

Mr. Secretary, I continue to be amazed at the challenge that you face. I sometimes wonder if we are really serious about carrying out the task that was given in your directive in the Homeland Security Act, which calls for development of that national assessment of threat and vulnerability, from which the Congress envisioned being able to then set priorities for funding, and also to allow the Department and the government generally to know where to allocate its resources in terms of protecting against terrorist attack.

We know the Presidential Directive Number Seven that you referred to postponed in my view the development of the identification of the critical infrastructure by at least, as I can read it, a year, because it says by the end of 2004, you are required to develop a plan to develop a strategy to identify, prioritize and protect critical infrastructure. I know Admiral Loy mentioned on one occasion that he thought this job ought to be done in a year. You were before this committee a few months ago. You said 5 years was a reasonable timetable.

When we look at the staff that you have available to you, I believe you have, if my numbers are correct, about 172 people on board, with the responsibility of trying to carry out this task of assessing and identifying our critical infrastructure. It just seems to me you have a task that really requires you to come in here and tell us what it is going to take to really get this job done in a reasonable period of time. I think I hear you saying to us that you are relying a lot on the ISACs and the voluntary cooperation of the private sector. That is good. That is important and I support you in that. But to really do what the Congress mandated in the Homeland Security Act in any reasonable time it seems to me it is going to require much greater commitment in terms of personnel to ever get this job done right.

I look just at the chemical industry, where you mentioned you plan to visit, or have identified 360 sites that you think are at high risk. I think you visited a few of those sites. I think I saw the numbers here earlier. You have a lot of work to do. I think I just heard you say you may not even be able to visit them all. You may rely on our state partners to do that. I am not even sure we have the authority to go look at those chemical sites, in terms of getting onto the premises and to evaluate them.

So you have that responsibility that seems to be virtually in a posture where you are going to have a very difficult time accomplishing it in any reasonable period of time. Then you have this responsibility of trying to solicit information from the private sector under the Protected Critical Infrastructure Information Program that you have just issued rules on, which is supposed to encourage industry to voluntarily tell you about their vulnerabilities. Yet all I am hearing is that industry is not satisfied with the regulations and are not sure they can trust this agency, so they do not know if they want to tell you anything or not. You have 32 employees dedicated to that program, with collecting that sensitive information. The budget is $3.9 million. My notes say that we have only received information from two companies and two associations to date.

So I really think that what I would like to hear from you regarding is, what do you really, in your gut, feel it is really going to take to do this job in a reasonable period of time? I know it is easy to say, well, I have my budget and this is all they have given me to do this job and I am going to try to do it the best I can and put the best face on it I can. But you are the person there that is in charge of all this. What I would like to have from you is some candid assessment regarding what you really need to do to get this job done in a reasonable period of time. I do not believe you have the staffing or the capability or the momentum or the support of the private sector yet to really ever get it done.

Mr. LISCOUSKI. I was hoping you would ask me that question, because this seems to me a perception we have to kill. The comment that I made last time, the first time I testified before you and said it was going to take us 5 years. I think that was taken entirely out of context. As I stated to Ms. Lofgren earlier, if we are doing our job right, we will continually revisit that process. The national assessment of our critical infrastructure is not just dependent upon what DHS is doing. It is clearly dependent upon what the state and local governments are doing; what the private sector is doing; and our other Federal agencies.

That process has been ongoing and we have created a list. We started this process back in March 2003 with 160 sites based upon the Liberty Shield list that we stood up for, the Iraqi war back in March. We have grown that list to over 1,700 high priority sites, and a total list of 33,000 sites and are adding to it daily. We are continuing to add to it because we get a lot of input from our state and local partners and the private sector on what is critical and what is not. That list is going to continue to grow and we are doing assessments, both economic as well as physical and cyber vulnerability assessments on all those.

It is a significant amount of work, but I think we are making very good progress on it. And yes, we are wholly dependent upon the cooperation we get from the private sector and state and local government. But I will tell you right now, the private sector, and this is another perception that if I do nothing today but tell you how much the private sector has stepped up to the plate to help us and had been doing this long before DHS came along, they have been doing a heck of a job. When I was in the private sector, we regularly cooperated with state and local law enforcement and the Federal Government to ensure that we could coordinate and communicate our vulnerabilities.

So, is there hesitation? Yes, there is hesitation because it is a trust model that we have to build, but I think we have a good stab at it. We are doing a very good thing with the congressionally enacted PCII. Are we getting a low response on it? I am thankful we are, because we have to do a lot of marketing and outreach to the private sector to ensure that we create the right model for them to ensure that they have the trust model for DHS, but I think the mechanism is there. The public comment period is still open, which I think will be open until mid–May.

I am not surprised we had a slow start out of the block. I was hoping for a slow start out of the blocks because I was fearful that we would get too much information to be able to handle it. Thank-fully, we have not. So I am very pleased with the mechanism we have created based upon congressional guidance to ensure that we could provide better protection for the private sector based upon their requests. I am confident that we will continue to grow that program over time.

Let me just go back to the beginning of the question, the very first question. I would like to take as much time with you personally to get you to understand our methodology in this process. The quantification of the metrics that we are trying to use to get output from the activities that we are engaged in is one in which there still has to be some research on. When we look at critical infrastructure protection, there are three major components against which activities have to be applied: physical, cyber and people. When we look at the vulnerabilities that are represented in those broad domains, we very aggressively identify the assets the vulnerabilities represented in those assets across each one of those common themes, from people, physical, as well as cyber. We put programs to be able to remediate and lower those vulnerabilities.

But the output and the measurement of what is being done, and to be candid with you, from a very private sector perspective, it is not just putting money into the program; it is making sure we have the right activities going on that can be consistently measurable and consistently applied over time, that the outputs can give us good indicators about what is being done, and not just what is being done and is not being done, but is it being done well enough to address the threat.

My vision on this, and this is going to take some time because the technology does not exist yet, is to create a national scorecard that allows us to identify where are we in a given sector; how well does it look. Those metrics and that quantification of these things, which has never really been done before in the security industry, is something with which we have been working in the academic and the private sector on identifying.

So to your point, my goals in terms of what we can do with this progress and this approach, is precisely to your point: identifying the key priorities; where do we need to put the funding stream; identifying who is doing what program and well, so with our Federal partners in HSPD–7, we are working with OMB to ensure that we get the metrics outputs to ensure that if a department has X million dollars placed against a specific requirement, that they are performing that. And "performing" does not mean are they spending money on time; "performing" means are they actually addressing the vulnerabilities and reducing vulnerabilities, and is there a measurable way that we can identify the outputs to ensure that we get some high degree of confidence of how well we are doing our programs.

So you are precisely on the right track in identifying what are the major priorities and challenges here, and that is exactly what we are addressing. It is not an overnight process. I am very prideful of the fact that what DHS has done over the past year has been something that we can measurably identify how we have addressed the vulnerabilities. It is more than just a few chemical sites. Across all the sectors, we have done a great job. The folks working for us, they have really worked hard and they are working hard. It is not about DHS. It is about working with all of our Federal partners and state and local.

So I think the things that we are doing, we can tell a good story. The biggest challenge we have is getting those metrics that allow us to in quantifiable terms measure the progress over time and identify the funding profile that you and your committee is so concerned about. We are doing the right thing and we can show what we are doing.

Mr. THORNBERRY. I thank the gentleman.

The gentleman from North Carolina, Mr. Etheridge.

Mr. ETHERIDGE. Thank you, Mr. Chairman.

A couple of questions. Mr. Liscouski, I am going to start with you because you talked about the risk assessment vulnerabilities. Let me ask you one question. You talked earlier about coordination with other Federal agencies. What is the nature of the coordination between DHS and other Federal and state agencies as it relates to developing the national plan to deal with the appropriate countermeasures to combat agri-terrorism, which deals with our food supply and a host of other areas. Can you give us an update on where that is?

Mr. LISCOUSKI. Yes, sir, I can. Recently, another Presidential Directive, HSPD–9 addressed bioterrorism and specifically the responsibilities in the agricultural industry that needs to be addressed by Agriculture and HHS and others that are partnering up in that space. We are coordinating that effort again under HSPD–7. I apologize for using these different directive numbers, but for critical infrastructure protection, to ensure that we have a holistic look on all the critical infrastructure sectors.

So in direct response, I would say that this is an area that we really need to give some very sharp focus to in terms of not just working with state and locals, but with the Federal agencies and ensuring that Agriculture and HHS would have respective leads in this space, and have the appropriate outreach, the appropriate mechanisms to ensure that the state and local governments are doing what they need to be doing, and they are facilitating that process.

Mr. ETHERIDGE. I do not want to interrupt you, but do you have a timeline?

Mr. LISCOUSKI. A timeline for?

Mr. ETHERIDGE. Completion, or at least a marker of where we can work from. This happens to be very important, because it fits what you talked about and deals with our food supply, not only here, but internationally in what we ship.

Mr. LISCOUSKI. That specific plan is in process. I cannot give you an accurate timeline at this point because that plan is in process. I am afraid whatever I tell you today is going to be inaccurate.

Mr. ETHERIDGE. Would you get back to me?

Mr. LISCOUSKI. I welcome the opportunity.

Mr. ETHERIDGE. Let me follow that up, because it follows that same thinking to some extent. I will not ask that question, but I will just put it in so you can follow later, because it deals with, several years ago we had a problem with our school lunches and the food supply and the problems that fell out from that. Let me ask what DHS is doing as it relates to, you said earlier, its products, facilities and people. We have seen in just the last couple of days what happened in Iraq with the bombing that took place there and a number of school children were killed. Can you tell me what is being done or what coordination is being done as it relates to our schools if a terrorist attack should hit?

Because we are looking at millions and millions of children in this country who go to school every day. Many are in buildings, but a large number now find themselves in what we call makeshift trailers. I hate to call attention to it, but there is a tremendous problem because they are isolated. What is being done? Has any assessment been done as to the comparability of protection within a brick and mortar building, to students who happen to find themselves, along with staff, in an isolated makeshift structure?

Mr. LISCOUSKI. Yes, sir. I can address that specifically. We have been working with the Department of Education, which as you know has a significant outreach capability broadly across the United States in K–12 as well as the university system. We met recently with Under Secretary McPherson and Deputy Under Secretary Price to incorporate them into our planning for HSPD–7, to directly ask them for their plan. In fact, we are working very collaboratively with them.

As you know, the education system is not identified as one of the critical infrastructure components of the Homeland Security Act, but we have the latitude of identifying other sectors as necessary. That sector is being addressed both directly and indirectly through my office's Soft Targets Branch. We regularly look at soft targets, which schools are one of, to address those specific types of requirements.

I cannot tell you specifically if we have looked at the analysis in the school environment of the impact of a trailer versus brick and mortar. I know we have done that in others.

Mr. ETHERIDGE. Would you follow up on that?

Mr. LISCOUSKI. I certainly would, sir.

Mr. ETHERIDGE. I appreciate it.

I know my time is almost up, but Mr. Newstrom, I have one for you. As Virginia's Chief Information Officer, what specific support would you expect from DHS or other Federal agencies, for that matter, if you computer system was attacked and was down for more than several days, and you were out of business, knowing that you have to have an off-site facility, but let's say it was damaged and out of space. Do you think the Federal Government could give you the expectations that you have? If so, what would you like to see us do?

Mr. NEWSTROM. I am not sure that we look toward the Federal Government in that specific scenario. We have established backup plans. We have established backup facilities. We have been redundant in those facilities and those plans. We work on and practice those plans. We also go to the private sector to ensure that we have not only internal Commonwealth resources that are backups and redundancies, we also have backup with the private sector.

From a Federal Government perspective, what I would see if there is a catastrophic outage in a region of the country. For instance, if there is an electrical outage; if there is a major telecom outage; I would ask that our resources work together very, very closely on that. But on the normal outages that you described, I think it is our responsibility to address those.

Mr. ETHERIDGE. Thank you, sir.

Thank you, Mr. Chairman.

Mr. THORNBERRY. I thank the gentleman.

The Gentlelady from the Virgin Islands, Mrs. Christensen.

Mrs. CHRISTENSEN. Thank you, Mr. Chairman.

I want to welcome our witnesses this morning. I have a concern, as I always do, about where health fits into the picture. My first question would go to Mr. Liscouski. We had a hearing or a briefing about a month ago on ISACs. At that time, health was not established. In the GAO report which we will hear about in a little while, health is not listed. I am assuming that is because it is not established.

Where are we? Is health not a priority in this area? Has something happened between the last briefing and today?

Mr. LISCOUSKI. Yes, ma'am. I think the ongoing work that is in progress there is that we have been working with the general health sector, both within HHS and with the other more diverse components, to establish their ISAC. It is a work in progress. It has not been listed by GAO, nor is it on our list because it is a work in progress. We do not believe we have consensus around who establishes what. I recall from my notes, and forgive me, I am not going to go through them, but I believe, as you well know, it is one of the more diverse communities in which to work. One of the challenges is establishing leadership in that community within one particular organization for the ISAC.

My sense is, and I would be happy to correct this later in subsequent research to get back to you in writing, but my sense is because it is so diverse we may wind up creating many sub-components of the ISAC, which may be aggregated up into one larger health ISAC. It is clearly on our radar screen as a priority, ma'am. So I just indulge you to not make a judgment that it is not a priority for us. It is.

Mrs. CHRISTENSEN. OK. Is there lead responsibility in the Department? Has that been identified? Or the divisional responsibility within DHS?

Mr. LISCOUSKI. The Infrastructure Coordination Division, of course, has the coordination requirement. Under HSPD–7, the sector-specific agency is HHS. Correct me if I am wrong on that. I should know this off-hand. But there is a sector-specific agency established under HSPD–7 for the health sector. We are working with them to ensure that we have the sector aligned and coordinated to establish the ISAC.

So to answer your question, yes, ma'am, there is a sector-specific agency responsibility for health.

Mrs. CHRISTENSEN. OK. Mr. Newstrom, is health fully integrated into NASCIO's program within the State of Virginia?

Mr. NEWSTROM. Health?

Mrs. CHRISTENSEN. The health sector.

Mr. NEWSTROM. It is fully coordinated and integrated right now. We are still working with HHS particularly on some of the communications capabilities through the states. They have a very good program within their sectors, but it is very programmatic. We are encouraging HHS particularly to focus through NCSD to channel their communications to the states. Our entire issue is fusing the information, rather than the stovepipes that Mr. Liscouski has talked about.

Mrs. CHRISTENSEN. OK.

Mr. Liscouski, you have said that there is a great reliance on the private sector in the development of the assessments, and 85 percent of the assets are owned by them. Are there any inherent conflicts between the objectives of the private sector and the objectives of government and the Department that have been identified, that had to be resolved as this process has been developed? And how did you resolve them?

Mr. LISCOUSKI. No, ma'am. I think the biggest challenge we have had is on the information-sharing side, with the vulnerability assessments back from the private sector and back into DHS. That is what is being addressed through the Protected Critical Infrastructure Information Act, the implementation of that.

As I pointed out earlier, to make a general statement, and you can always find exceptions to this, but the private sector is stepping up to the plate of their responsibilities to ensure that they understand what is vulnerable for them and in sharing that with state and local governments, those who are responsible for protecting, and ultimately with DHS. So again, just to reiterate, I believe the one challenge which I think we are addressing is the information sharing between the private sector and DHS.

Mrs. CHRISTENSEN. OK. My last question, and you have probably been asked this both at the budget hearings and in several different ways here today, but you said you do not have sufficient bandwidth to do the assessment. That is why the private sector is really responsible for doing that and getting that information to you. Other testimony says that DHS has limited resources. We have seen very close progress. A lot of the questions have been around when is the assessment going to be in place. You have said the synchronizing and harmonizing of disparate parts is something that is still ongoing, and getting a complete situational awareness picture is something that you are still working on.

The Department has the primary responsibility for the protection of our critical infrastructure. I am just concerned that if these limitations exist and that we are not getting the full picture of what you really need in your budget to ensure that you are able to carry out the mandate of your directive and the Department.

Mr. LISCOUSKI. No, ma'am. I need to correct your statement. I do not mean to be presumptuous, but the comment I made about sufficient bandwidth is not relevant to do we have the capability and the necessary resources. We do. You could give me more money. It is not a money issue. What it is is that the information that has to be collected is not about what DHS can do. Nor would I suggest to you that this is a responsible role for the Federal Government to do it all. The Federal Government, and this is a national problem, you would not create a mechanism as big as you would need to collect all the information you want.

So the appropriate approach is the one that was created with the Department of Homeland Security, which is clearly a coordination-collaborative approach with our state and local partners, with other

Federal agencies to ensure that we can get them to do what they have to do. That is precisely what we are doing. It is leverage. It is not about bandwidth, necessarily. What I meant about bandwidth is all the things that would scope into that, time, and the enormity of the complexity of the task.

This is not, do we need to have more resources at the Federal Government level to do all this work. This is about working with our partners and our stakeholders to get them to do what they need to be doing. That is the essence of this. At the end of the day, the questions and the concerns we need to be addressing here are developing and creating consistent sustainable programs which are effective and measurable over time, that can answer the big questions of, are we protecting what we need to be protecting? And are we really doing it well?

That is the process we are developing. Again, level-setting the expectations here, this is not going to happen overnight. If I had a magic wand, if you all could tell me if there is one thing you could give to me that would allow me to do my job better, it would have to be a want that I could just broadly push across the United States and say, it's protected. But it is a process. It is a process because our economic system and everything we have built in this country is predicated on being open. Our openness which is our greatest strength is our single biggest vulnerability.

So it is an enormous thing to address. It is not about what DHS can do. It is about mobilizing the American public. It is about engaging with the private sector and the state and local governments to ensure that we all know what we have to do and we can measure it in a way that we can tell with confidence that we are doing the right thing.

So again, I just want to correct a misperception I have created, which is not about do I have enough resources. It is about we all have to mobilize at all the levels of Federal and state and local governments to do the right thing.

Mr. THORNBERRY. I thank the gentlelady.

The new member of the committee, the gentleman from Kentucky. Welcome. You are recognized for 5 minutes.

Mr. CHANDLER. Thank you, Mr. Chairman. It is nice to be here.

Mr. Liscouski, thank you for your testimony. Thank you for being here today. I am interested in some information regarding our efforts to protect and secure critical Federal facilities. For the past several decades in Central Kentucky, our citizens have lived next to a potentially dangerous chemical weapons stockpile. This is the Bluegrass Army Depot near Richmond, Kentucky. It contains well over 500 tons of chemical weapons, nerve gas, mustard gas, that sort of thing.

In 1988, in its environmental impact statement, the Department of the Army identified that in a worst-case scenario, an incident that would occur at this depot could result in plus or minus 15,000 fatalities in our area. So you can imagine that this is something of great concern to us.

What I would like to know is what type of information-sharing activities are occurring right now between the Department of Homeland Security, the Department of Defense, state and local governments, first responders, all those folks, to ensure that we prevent and are prepared to respond to an accident or a deliberate attack on facilities like this one, Federal critical infrastructures.

Mr. LISCOUSKI. Sir, you pointed out a key stakeholder in your question, and it is the Department of Defense which has responsibility for the defense industrial base and the supply chain that feeds that, and that is clearly a component of that. But we partner up very closely with DOD. They have a very robust capability on critical infrastructure as it relates to their facilities. Their partnership with state and local governments is something we have integrated our efforts with, as well as our response and recovery efforts.

I can speak to them at a top level. As you well know, that is outside my directorate, but working with state and local first responders under the directorate for EP &R, I do not know if exercises have been held directly in that jurisdiction, but I can get back to you on that.

Mr. CHANDLER. If you would, please do. That was another one of my questions, whether exercises would be held. I do not believe that they have been. I am very curious to know whether there are plans in the works to hold exercises to make sure that our folks are ready.

Mr. LISCOUSKI. Yes, sir. I would be happy to get back to you on that.

Mr. CHANDLER. I appreciate that very much. You all are working with the Department of Defense, though, on these sorts of issues; working very closely, but as I understand it, you are not aware of precisely what has been going on.

Mr. LISCOUSKI. At that particular site, sir, I do not know. I cannot tell you that specifically. I would be happy to get back to you on that one.

Mr. CHANDLER. OK. If I may just add one other question. You may want to get back to me on this as well. If there was an attack on that depot, we have already in place, and this is a team that pre-dated the creation of the Department of Homeland Security. It is the 41st Weapons of Mass Destruction Civil Support Team. It is based in Louisville, Kentucky. It is currently responsible for responding to a disaster at that facility. I am interested in knowing whether DHS has gone back to that team and checked on working out some sort of information-sharing arrangement with them.

Mr. LISCOUSKI. Sir, I will have to get back to you on that.

Mr. CHANDLER. OK.

Mr. LISCOUSKI. Thank you.

Mr. CHANDLER. Thank you very much.

Mr. THORNBERRY. I thank the gentleman.

The gentleman from Maryland.

Mr. CARDIN. Thank you very much, Mr. Chairman.

Let me thank both our witnesses for their testimony here today. I find it very informative and very helpful.

I want to talk about the National Capital Region for one moment, if I might. Tomorrow, the House of Representatives is going to be talking about the continuity of the House of Representatives in the event of an attack against us. I have many concerns about how well we are prepared in the National Capital Region itself. I know that there are committees that have worked on it. I know there is cooperation between Maryland and Virginia and the District of Columbia and the Federal Government. I am concerned somewhat that I believe the region that has been included in the studies are somewhat small, with a restricted number of counties within Maryland and Virginia. I represent Annapolis. I represent Baltimore. I know that there is an episode that occurs at a chemical plant in Baltimore and it will have an impact on the National Capital Region. I know that on any given day trying to get out of the nation's capital is a challenge. If we have a national emergency, it is going to be impossible.

I just want to get some assurances from you that clearly progress is being made here as to how we can prepared. We know that this is the seat of government. We know that it has been a target of terrorist attacks. We know the tremendous interests of this area in disrupting our government. So can you just share with us as to what special considerations are being made in regard to the National Capital Region and how it is affecting the surrounding jurisdictions beyond just the immediate counties in Virginia and Maryland that are directly working with you.

Mr. LISCOUSKI. Sir, I appreciate your question. I am going to have to defer to Under Secretary Mike Brown who is responsible for the response requirements through the NCR. I can tell you just based upon my level of understanding and engaging on the critical infrastructure protection side, that I have knowledge that there are regular exercises being conducted throughout this region, which address some of the concerns you have. But to give you more confidence, I just request to defer that to Under Secretary Brown for a response.

Mr. CARDIN. Let me bring you into this discussion, because you are making assessments of the nation's infrastructure sensitivities and priorities. I would just urge you that the Federal facilities located in the National Capital Region and surrounding areas are particularly vulnerable. The stress on local governments is particularly great. The chemical plants in Baltimore present an extra challenge. All chemical plants present challenges. The fact that it is located close to the nation's capital makes it an even more sensitive target. The Federal facilities located in Annapolis or located along I–95 close to the nation's capital are particularly vulnerable because of location.

As you are making your national needs assessment, is location, those types of considerations, going into the equation as to the type of fences that we need to put in place?

Mr. LISCOUSKI. Yes, sir, it is. We have been doing a lot of work, as you are probably well aware, with state and locals here in the National Capital Region, doing the assessments for the various infrastructure components to include the Federal facilities. We have I think a robust capability there in understanding not just what we have to do to protect, but the actual protection of those facilities has been equally as robust.

So yes, sir, to answer your question, we are working very closely with the state and locals. We understand that there are some limitations. We are trying to supplant those limitations through the ODP grant process, but we are working very closely with them. So from a protection standpoint, we have very good clarity around the vulnerabilities that are here, as well as the protection requirements that are needed to mitigate those vulnerabilities.

Mr. CARDIN. Did you want to respond?

Mr. NEWSTROM. Congressman, in my written remarks I address the NCR specifically. In addition to what DHS is doing, the Governors of Virginia and Maryland and the Mayor of the District of Columbia have met together on this specific subject. In fact, because of funding through and by DHS, we have an initiative called the Urban Area Security Initiative, which specifically focuses on the National Capital Region and first responders. We have come a long way since 9–11.

Mr. CARDIN. I was just going to point out that the concern we have with that is it s the restricted jurisdictions that can participate within Maryland and Virginia. When you look at trying to evacuate people from the nation's capital, you need to look beyond just the immediate counties in Maryland and Virginia. As you look at protecting infrastructures, you need to also look beyond those counties.

If you live in Anne Arundel County, Maryland, where many people commute into Washington, D.C. or you live in Frederick County, you are very much impacted also. We are concerned that there is a limited interest and it needs to be expanded.

Let me let you continue on that.

Mr. NEWSTROM. Congressman, you are absolutely right. I could not agree with you more. In fact, the initial steps were originally around communications and the lack of ability by policing entities from the different jurisdictions to be able to communicate during and after 9–11, including the military. So that was addressed very, very early. But around transportation and the issues that you bring up, we are still in the infancy stages of trying to define that.

Mr. CARDIN. I would just urge you to give it a higher priority. Thank you, Mr. Chairman.

Mr. NEWSTROM. Yes, sir.

Mr. THORNBERRY. I thank the gentleman.

The gentleman from Washington.

Mr. DICKS. Thank you.

Mr. Liscouski, I am very concerned about something. It is my understanding that your directorate has compiled a critical asset target list for each state, and forwarded that list to each state's primary point of contact to begin planning security enhancement activities. I have reviewed this list of critical assets in Washington State and I am deeply concerned by several obvious omissions that fit well within the criteria presented.

I have discussed this issue with my state's homeland security adviser, who has told me that there was very little opportunity for comments and revisions coming from the state and local level. It is absolutely imperative that a list of critical infrastructure be developed. I could do this. I think any member of Congress could sit down in about 10 minutes in their own district and write down a list of critical infrastructure. If you have 170 people down there, I cannot understand why it is taking so long to get this job done. I worry about the gaps.

When you have a list that does not. . .you have the Seahawk Stadium, you have the Husky Stadium, but you do not have Safeco

Field, the Tacoma Dome, the Port of Seattle, the Port of Tacoma, Grand Coulee Dam. . .talk about a national icon. . .the Boeing Company and Microsoft. None of them are on the list, including the Puget Sound Naval Shipyard in my hometown of Bremerton, Washington, which overhauls and repairs every major nuclear ship on the West Coast; the Trident Submarine base, we have nuclear missiles and nuclear weapons.

What is going on here? This list that I saw is the most pathetic exercise I have ever seen since I have been up here. There are a lot of pathetic things I have seen in 28 years in Congress, but this is the worst I have ever seen. I could have done this myself and done a better job. I do not understand who is doing this. Who are they talking to? This is serious. It is not getting done and I am very concerned about it. Can you give me some assurance that we are going to get this thing straightened out, that somebody will talk to the people in the State of Washington? To General Lowenberg who is the Governor's assistant, and get a credible list of things put on this thing? Why is this not happening?

Mr. LISCOUSKI. Thank you, Mr. Dicks. I am a little surprised at the characterization from the homeland security adviser that he has not been contacted or has not had any input. In fact, the purpose of sharing that list is to solicit the input.

Mr. DICKS. But the list has already been put out. Here it is. They should have consulted with them before they put out the list.

Mr. LISCOUSKI. I will certainly get back to you to find out if they had or had not been consulted.

Mr. DICKS. I have the list right here. None of these things are on there. This is like the crown jewels of Washington State. Every one of them is missing from this list. I just cannot believe that this is happening.

Mr. LISCOUSKI. Mr. Dicks, I just want to caution. We typically do not publicly disclose the assets on that list. So to talk about it in any degree of fidelity here, I would suggest—.

Mr. DICKS. None of them are on there, so I have not discussed anything that is on there.

Mr. LISCOUSKI. To my point, I would be happy to discuss with you in a separate setting—.

Mr. DICKS. To discuss the things that are not on there?

Mr. LISCOUSKI. Sir, to my point, I would be happy to discuss with you in a private setting where we can talk about specifically what is on the list and what is not on the list, but I do not think this is the appropriate forum right now.

Mr. DICKS. Can you answer this question? Let's go to the process. Why is this thing so screwed up? With all due respect, I do not get any sense of urgency here.

Mr. LISCOUSKI. There is a significant sense of urgency, sir. Again, without commenting on the specifics of that list, I will go back and review the process and I would be happy to sit down with you and talk to you about how that list was developed. If there are gaps, we would be happy to correct them. The mandate is for my folks to make sure we absolutely engage with all the respective stakeholders at the state and local sectors to ensure we have it right. I will be happy to review it and get back to you, sir.

Mr. CAMP. Would the gentleman yield just for a brief moment?

Mr. DICKS. Yes, I yield.

Mr. CAMP. The subcommittee did hold a classified briefing where the Secretary did bring the full list. It was available for all members to review who attended that briefing. I would be happy to work with you to try to make sure so that not only there, but other places—.

Mr. DICKS. The list that we have right here, this is not—.

Mr. CAMP. It is classified, so we did not take any paper out of the room, but I know that Ms. Sanchez was there and it might have been difficult for other members' schedules to attend that particular classified briefing. I know the Chairman was there and others. But we had an opportunity to review this list and we all looked at various assets from our states and made comments.

Mr. DICKS. Apparently we were only given 24 hours notice of that, but I appreciate the fact that you did it. I do not want to be critical of that.

Mr. CAMP. We did have more notice than that because we worked on it for a long time to get it put together. So I would dispute that it was only 24 hours notice, frankly.

Mr. DICKS. That is the actual time of the meeting.

Mr. CAMP. Yes.

Ms. SANCHEZ. Would the gentleman yield?

Mr. DICKS. Yes, I yield. I am just worried about this.

Mr. CAMP. We did have an opportunity to look at that.

That is just my point. Thank you.

Mr. DICKS. OK. I yield.

Ms. SANCHEZ. We are trying, I believe, to set up another meeting with more notice to do the same thing. It is a classified list. There are things that are omitted from that list, even from my own district. You only get to look at it when you are in there, but hopefully you can attend the meeting; you can take a look at what is really on the list. I do not know if that list is what is the list that we took a look at when we were in the private meeting.

Mr. DICKS. Maybe there is a separate list that we were not told about. This is what I was presented. The reason I am concerned is there are a lot of things that should be on that list that are not on there.

Mr. LISCOUSKI. Sir, maybe if I can just have one final comment, without drawing this out. The states were required to submit their list, sir, so I suspect if we did not receive their input, and again I will go back to our group to address this, but there are a couple of different reasons as to why the list you may have, it may be old or out of date, I am not quite sure what, but we did not do anything without the state's input, sir.

Mr. THORNBERRY. Does the gentleman yield back?

Mr. DICKS. Just for one second. The list we have is the list that was given to the Adjutant General. He was quite concerned about it and made that clear and made it clear to us, the members of the delegation for the State of Washington, that he was quite upset about it. Washington State has been as forward-leaning as any state that I know of. They have done a complete statewide plan. In that plan, it talked about all these other issues that I mentioned that are not on this list. So to me, I just hope we can get this straightened out.

Mr. THORNBERRY. I thank the gentleman. This is obviously not an issue before my subcommittee. It is Mr. Camp's subcommittee. When we are talking about information sharing, if there are classified lists that are floating around in a way that classified information is not supposed to be handled, I am a little concerned about that.

Mr. CAMP. Would the Chairman yield?

Mr. THORNBERRY. Sure.

Mr. CAMP. I would be very concerned if the Adjutant General is sharing that list in that format in an unclassified way, frankly. That is not appropriate. So if that is the way that information is getting out, I would question its accuracy and I would certainly question the process.

Mr. DICKS. It was not presented to him in a classified format.

Mr. CAMP. It is probably not the correct list. So I think what we need to do is have another classified briefing.

Mr. DICKS. We have to sort this out. I will glad to apologize to anyone if this is not the list, because when I saw this list I frankly was outraged, as you can tell.

Mr. CAMP. The purpose of the meeting was to make sure that members did have an opportunity to review lists from their states, because we do think that it was in a classified setting inside the skiff so that it was a confidential meeting. I will be glad to work with the gentleman to try to set up an opportunity.

Mr. DICKS. Let me just for the record, the person who presented this list to the state was James McDonnell, Protective Security Division, U.S. Department of Homeland Security.

Mr. CAMP. It may not be a complete listing of all of the assets on the classified list. We will get to the bottom of it.

Thank you, Mr. Chairman.

Mr. DICKS. I appreciate the gentleman's help.

Mr. THORNBERRY. We are ready to move to the second panel. Does the gentlelady from Texas have questions she would like to ask of this panel?

Ms. JACKSON-LEE. Yes, I do.

Mr. THORNBERRY. The gentlelady is recognized.

Ms. JACKSON-LEE. Thank you very much, Mr. Chairman. I was in a hearing with both the Chairpersons and the Chairman of the full committee that I hope we will have, and that is with Secretary Powell and Governor Ridge on the request for an extension of the biometric passport. So I apologize to the witnesses for my delay, but let me just ask one pointed question to the Assistant Secretary.

Just for your information, I know many of us come from areas that have their own critical infrastructure, but coming from Houston, Texas obviously the refineries and the chemical plants are very well known. In fact, in the last four to six weeks, we had yet another explosion in the area that impacted neighborhoods and impacted people. We are grateful that it was a technical or an infraction that had nothing to do with terrorism, but you can imagine the sensitivity to this issue.

So let me just cite specifically what we seek. I think that you may be aware of a recent news program that highlighted the conditions of chemical plants, and I might say the outrageous condition of chemical plants, open gates, lack of guards, dilapidated fences, all allegedly protecting chemicals that could potentially kill or injure tens of thousands or even millions of people nearby.

We know the ISACs are working on communication. I understand that DHS is developing a best practices, but it is hard to imagine that every plant manager does not already know or that we cannot simply get out a manifesto to every plant manager by way of inventorying all of these plants wherever they might be, that closing the gates around tanks of chlorine gas a mile from a school is a best practice.

So my question is, how can we secure the homeland when even these simple tasks are not being done? One, has your particular area done the risk assessment that many of us have been calling on for a long, long, long time? Have you done that in the context of getting out the simple to-dos, such as closing fences, fixing gaping holes in fences, providing some kind of lock system, trained security personnel? And do we have a manifesto of sorts, a document that can easily be understood by the myriad of chemical operations around the country?

I can assure you that we in Houston and the parameters of our area have been faced with explosions throughout our lifetimes. We have been fortunate that it has not been the massive catastrophes that a terrorist act could bring about, but we have lost lives. So I am very concerned, one, that we still sit here in 2004 without a risk assessment. I would ask you if you could respond to that, as well as any simple tasks that have been given to these operators of these plants that they could be implementing as we speak.

I thank the distinguished Chairman.

Mr. LISCOUSKI. Yes, ma'am. Thank you. I addressed this earlier and I would be more than happy to do it again when we talk about the national assessment.

Ms. JACKSON-LEE. I thank you for your indulgence.

Mr. LISCOUSKI. This notion of a national assessment is something we have discussed many times. It is ongoing. We are making significant progress in compiling our national asset database. As I mentioned earlier, when DHS was first created back in March of 2003, we had started off with a list of about 160 critical sites in the United States that we thought were the high priority targets. We quickly grew that to 1,700. Out of a list of 33,000 assets that we have currently identified, we are still getting information back from the state and locals about what their priorities are and what should be on that list. That list is growing.

We are prioritizing those activities. As it specifically relates to the chemical sector, we have identified out of the 4,012 sites around the United States that we believe are those that require the top tier. Not top tier, but of the 4,000 sites we have identified, this year alone we are addressing the 360 sites around the United States that need to address their security. We are addressing that in a variety of ways.

First of all, let me just qualify. The issue here is not just a private sector problem, but this is a state and local government and private sector problem. It needs to be a totally integrated plan. We are working with state and local authorities, as well as the private sector to put out best practices. To that end, we have done a variety of things.

We have put out common vulnerability assessments and shared those with best practices perspectives.

Ms. JACKSON-LEE. Mr. Secretary, may I do this, because as you indicated I came in and you had already indicated that. Let me just be pointed.

Mr. LISCOUSKI. Sure.

Ms. JACKSON-LEE. Have you in any way secured the transcript of that program, 60 Minutes? Have you visited any of those plants, because they seem to be the worst-case circumstances. If I may make a comparison, though it is probably an unreal comparison, over the last 24 hours we had a number of bombings at Iraqi police stations. That seems to be a notable target. Maybe our allies and Coalition forces should be having an inventory of police stations, knowing that they are targets.

We know that chemical plants can be targets. There are atrocious activities going on, maybe for lack of direction. Have you gone out into the field and visited these plants? When you say "ongoing risk assessment," I can only say to you that "ongoing" is positive to the effect that we always believe we should continue to learn, but it is not positive from the perspective of the crisis of terrorism in this country. So when will we finish the risk assessment? Have you been to these plants and given them any direction?

Mr. LISCOUSKI. Yes, ma'am, we have.

Ms. JACKSON-LEE. I am sorry?

Mr. LISCOUSKI. Yes, ma'am, we have been to the plants. We have been to plants specifically in your jurisdiction, in fact, and I would be happy to share those details with you in a different venue other than this. We have been very aggressive about the prioritization of chemical plants. It is a top priority for us. We recognize the vulnerabilities. We are working with the industries, state and local governments, as I pointed out. We have buffer zone protection plants in place. We have shared best practices for vulnerability assessments. We have shared common characteristics of terrorist operational patterns with both the industry and state and local governments.

So I am quite confident that we are addressing it. To your point, we are in a continuous improvement process. Unfortunately, those remarks get taken out of place. You always ask me, am I satisfied? I am never satisfied. I think it is one of the reasons I got this job. It is because you never want to be satisfied with where you were. We never want to become complacent.

So we are in a continuous improvement mode. Will we ever be finished? We are going to continuously improve our ability to provide protection in this country of ours, because this is an incredibly complex problem. It is not just about what the plants are doing. It is how are the groups themselves evolving their techniques and their capabilities? So this is a multi-dimensional process. This is not just one which becomes static to say, put up a 12-foot-high fence and you have security, because we know that terrorists can get a 15-foot-high ladder.

So we are continuously looking at what we need to be doing here to improve security. I know you are very sensitive to that. I appreciate your comments. I would be happy to share with you with more fidelity about what we are doing. I know we have done that many times with the staff up here. If you have not had the benefit of a briefing, I would offer that to you.

Ms. JACKSON-LEE. Mr. Chairman, I thank you very much. I will accept your offer, Mr. Secretary. I would like to talk specifically about the region and what you have done in that area. I thank you very much.

Mr. LISCOUSKI. Terrific. Thank you.

Mr. THORNBERRY. I thank the gentlelady. I thank both of our witnesses.

I am going to submit my questions in writing to the witnesses. Mr. Liscouski, if we could have a similar agreement with you as we had before, and that is a real effort to try to get answers to written questions in two weeks. I understand it is not completely within your control, but if you can help push on your end, I think it will help relations with all members. We will also try to limit the number of questions.

Secretary Newstrom, let me also encourage you on behalf of your organization to continue to discuss with us not just how much we have improved, but what yet needs to be improving, because it is only by identifying those areas that we still need to make progress on, giving little pushes here and there, that we can, as Mr. Liscouski said, though we will never be satisfied, we can continue to improve. I think you hit on some key points in your testimony.

With that, let me thank both these witnesses. You are both excused. We will go ahead and bring up the next witnesses. We should have votes starting soon, but we will press on until the bells make us recess.

So thank you both. You are both excused.

Mr. NEWSTROM. Thank you.

Mr. THORNBERRY. Let me thank the members of the second panel for your patience. Obviously, there is a lot of interest in this issue. I have no doubt we will need to recess for votes here in a moment and come back. We will do that.

As you all are getting situated, I will introduce our next panel, which includes Mr. Robert Dacey, director, information security issues for the General Accounting Office; our former colleague, Hon. Dave McCurdy, executive director of Internet Security Alliance; and Ms. Diane VanDe Hei, vice chair, Information Sharing and Analysis Center Council.

Mr. Dacey, I think you are first. Would you like to submit a summary of your statement before we go and vote? If you could do that within 5 or 6 minutes, then we will go ahead and do that, and then we will have to come back for the other witnesses. Thank you again for being here, and you are recognized.

STATEMENT OF ROBERT DACEY, DIRECTOR, INFORMATION SECURITY ISSUES, GENERAL ACCOUNTING OFFICE

Mr. DACEY. Thank you, Mr. Chairman and members of the subcommittee. I am pleased to be here today to discuss the status of ISACs, including the initial results of our ongoing review which we are performing at the request of the subcommittees. As you requested, I will briefly summarize my written statement.

Beginning with PDD–63, Federal policy has encouraged the voluntary creation of ISACs as key information-sharing mechanisms for the private sector entities and state and local governments that own and operate most of the nation's critical infrastructures, and for the Federal Government. Further, Federal policy established specific infrastructure protection responsibilities for the Department of Homeland Security and other Federal agencies.

Although their missions are similar, the current ISACs were established and developed based upon the unique characteristics and needs of their individual sectors. Consequently, they operate under different management and operational structures and have different operational capabilities, which are summarized in our written statement and include, number one, various business models such as private entities, parts of associations, or a partnership with the Federal Government. Many also use contractors to support their operations. They also vary in the nature of the hazards that are covered, such as cyber, physical or all hazards, which would also include natural events.

The second major point is the various funding mechanisms that exist. They may be funded through special fee-for-service activities including tiered levels, association sponsorship, Federal grants, or voluntary or in-kind operations by the participants.

The third major difference is the models or methods by which they share information. While most have electronic information shared via email and Web sites, some of which are secured, others have regular conference calls for their members, and some have established facilities for quickly organizing crisis conference discussions.

DHS and the sector-specific Federal agencies have undertaken a number of efforts to support the ISACs and to build the public-private partnership called for in Federal CIB policy. Mr. Liscouski earlier today discussed at some great length the efforts being taken by the Department.

In addition, the sector-specific agencies are also taking actions, including funding, to help ISACs increase their memberships and improve their analytical and communications capabilities. Nonetheless, according to ISAC representatives and the ISAC Council which is also represented on this panel, a number of challenges remain to their successful establishment, operation and partnership with DHS and other Federal agencies. These challenges include increasing the percentage of sector entities that are members of the ISACs; two, building trusted relationships and processes to facilitate information sharing; three, overcoming barriers to information sharing; four, clarifying roles and responsibilities of the various governmental and private sector entities involved in protecting our critical infrastructures; next, funding ISAC operations and activities; and utilizing sector expertise.

According to a DHS official, these issues are being considered by the Department and should be clarified with the development of a plan that will lay out the current relationships, goals for improving them, and methods for measuring progress. To help ensure that a comprehensive and trusted information-sharing process is established, it will be important to consider input from all appropriate stakeholders and to agree upon the respective roles, responsibilities, relationships and expectations of the parties.

Mr. Chairman, this concludes my statement. I will be pleased to answer any questions that you or other members of the subcommittee may have.

[The statement of Mr. Dacey follows:]

PREPARED STATEMENT OF ROBERT F. DACEY

UNITED STATES GENGERAL ACCOUNTING OFFICE

CRITICAL INFRASTRUCTURE PROTECTION

ESTABLISHING EFFECTIVE INFORMATION SHARING WITH INFRASTRUCTURE SECTORS

Messrs. Chairmen and Members of the Subcommittees:

I am pleased to be here today to discuss the status of private-sector information sharing and analysis centers (ISACs) and their efforts to help protect our nation's critical infrastructures. Critical infrastructure protection (CIP) activities called for in federal policy and law are intended to enhance the security of cyber and physical, public and private infrastructures that are essential to national security, national economic security, or national public health and safety. Beginning with Presidential Decision Directive 63 (PDD 63) issued in May 1998, federal policy has encouraged the voluntary creation of ISACs to facilitate private-sector participation and serve as mechanisms for gathering, analyzing, and appropriately sanitizing and disseminating information to and from infrastructure sectors and the federal government. Subsequent federal CIP policy, including several national strategies, continued to emphasize the importance of the ISACs and their information-sharing functions.[1] Further, CIP policy has established specific responsibilities for the Department of Homeland Security (DHS) and other federal agencies with respect to public-private collaboration to help protect private infrastructure sectors.

In my testimony today, I will discuss the management and operational structures used by the ISACs, including their estimated sector participation, business and funding models, and information sharing and analysis mechanisms. I will then discuss activities by DHS and other federal agencies with responsibilities for specific infrastructure sectors to interact and support the ISACs. Lastly, I will discuss some of the ISAC identified challenges to and successful practices for their establishment, operation, and partnership with the federal government.

As agreed, this testimony includes initial results of our ongoing analysis of private-sector ISACs, which was requested by your subcommittees. In conducting this work, we contacted officials for the 15 different ISAC organizations that had been established at the time of our review: Chemical, Electricity, Energy, Emergency Management and Response, Financial Services, Food, Information Technology, Multi-State, Public Transit, Real Estate, Research and Education, Surface Transportation, Telecommunications, Highway, and Water. Through structured interviews with these officials, we obtained and analyzed information to describe the ISACs' current organization and operational models, funding mechanisms, sector representation and membership criteria, as well as their challenges and successful practices in establishing effective information-sharing relationships within their sectors and with the federal government. We also contacted officials of the Healthcare Sector Coordinating Council to discuss their efforts to establish an ISAC for the healthcare sector. Further, we contacted officials of the ISAC Council, which was created by 11 ISACs to address common issues, and obtained and analyzed its series of white papers on a range of ISAC-related issues and challenges. Within the federal government, we obtained and analyzed information on efforts to work with the private-sector by DHS and other agencies assigned responsibilities for specific industry sectors, including the Departments of Agriculture, Energy, Health and Human Services, and the Treasury and the Environmental Protection Agency. We did not validate the accuracy of the data provided by the ISACs, DHS, or other agencies. We performed our work from November 2003 to April 2004, in accordance with generally accepted government auditing standards.

Results in Brief

[1] The White House, The National Strategy to Secure Cyberspace (Washington, D.C.: February 2003); The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (Washington, D.C.: February 2003); and Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection (Washington, D.C.: Dec. 17, 2003).

Beginning with PDD 63, federal policy has encouraged the voluntary creation of ISACs as key information-sharing mechanisms between the federal government and critical infrastructures. While PDD 63 suggested certain ISAC activities, CIP policy has essentially left the actual design and function of the ISACs to the entities that formed them. As a result, although their overall missions are similar, the current ISACs were established and developed based on the unique characteristics and needs of their individual sectors. They operate under different management and operational structures and, among other things, have different business models and funding mechanisms. For example, most are managed or operated as private entities with some, such as the Water and Chemical ISACs, part of associations that represent their sectors. Others have partnered with government agencies, such as the Telecommunications ISAC, which is a government-industry operational and collaborative body sponsored by DHS's National Communications Systems/ National Coordinating Center (NCC). Different funding mechanisms used by the ISACs include fee-for-service, association sponsorship, federal grants, and/or voluntary or in-kind operations by ISAC participants. Examples of fee-for-service funding include the Financial Services, Information Technology, and Water ISACs that offer tiered memberships with fees based on the level of service provided.

DHS and the sector-specific agencies have undertaken a number of efforts to address the public-private partnership called for by federal CIP policy and continue to work on their cooperation and interaction with the ISACs and with each other. For example, in January 2004, DHS held a 2-day conference to describe the information they are analyzing and its use in the partnership with the private sector and to discuss information sharing between the federal government and the private sector. Also, in February, the department established the Protected Critical Infrastructure Information (PCII) Program that enables the private sector to voluntarily submit infrastructure information to the government, which can be protected from disclosure according to provisions of the Critical Infrastructure Information Act of 2002.

According to ISAC representatives and a council that represents many of them, a number of challenges remain to their successful establishment, operation, and partnership with DHS and other federal agencies. These challenges include increasing the percentage of sector entities that are members of the ISACs; building trusted relationships and processes to facilitate information sharing; overcoming barriers to information sharing, including the sensitivity of the information, legal limits on disclosure (such as Privacy Act limitations on disclosure of personally identifiable information), and contractual and business limits on how and when information is disclosed; clarifying the roles and responsibilities of the various government and private sector entities involved in protecting the critical infrastructures; and funding ISAC operations and activities. According to a DHS official, these issues are being considered and should be clarified through the department's development of a plan that documents the current information-sharing relationships between DHS, the ISACs, and other agencies; goals for improving that information sharing relationship; and methods for measuring progress.

Background

As reliance on our nation's critical infrastructures grows, so do the potential threats and attacks that could disrupt critical systems and operations. In response to the potential consequences, federal awareness of the importance of securing our nation's critical infrastructures, which underpin our society, economy, and national security, has been evolving since the mid-1990s. For example, issued in 1998, Presidential Decision Directive 63 (PDD 63) described the federal government's strategy for cooperative efforts with state and local governments and the private sector to protect the systems that are essential to the minimum operations of the economy and the government from physical and cyber attack. In 2002, the Homeland Security Act created the Department of Homeland Security, which was given responsibility for developing a national plan; recommending measures to protect the critical infrastructure; and collecting, analyzing, and disseminating information to government and private-sector entities to deter, prevent and respond to terrorist attacks. More recently, issued in December 2003, HSPD–7 defined federal responsibilities for critical infrastructure protection, superseding PDD 63.

CIP Policy Has Continued to Evolve

Federal awareness of the importance of securing our nation's critical infrastructures has continued to evolve since the mid-1990s. Over the years, a variety of working groups has been formed, special reports written, federal policies issued, and organizations created to address the issues that have been raised. Key documents that have shaped the development of the federal government's CIP policy include:

- Presidential Decision Directive 63 (PDD 63),

- The Homeland Security Act of 2002,
- The *National Strategies for Homeland Security,* to *Secure Cyberspace* and *for the Physical Protection of Critical Infrastructures and Key Assets,* and
- Homeland Security Presidential Directives 7 (HSPD–7) and 9 (HSPD–9).

Presidential Decision Directive 63 Established an Initial CIP Strategy

In 1998, the President issued PDD 63, which described a strategy for cooperative efforts by government and the private-sector to protect the physical and cyber-based systems essential to the minimum operations of the economy and the government. PDD 63 called for a range of actions that were intended to improve federal agency security programs, improve the nation's ability to detect and respond to serious computer-based and physical attacks, and establish a partnership between the government and the private-sector. Although superseded in December 2003 by HSPD–7, PDD 63 provided the foundation for the development of the current sector based CIP approach.

To accomplish its goals, PDD 63 established and designated organizations to provide central coordination and support, including the National Infrastructure Protection Center (NIPC), an organization within the FBI, which was expanded to address national-level threat assessment, warning, vulnerability, and law enforcement investigation and response.

To ensure the coverage of critical sectors, PDD 63 identified eight infrastructures and five functions. For each of the infrastructures and functions, the directive designated lead federal agencies, referred to as sector liaisons, to work with their counterparts in the private-sector, referred to as sector coordinators. Among other responsibilities, PDD 63 stated that sector liaisons should identify and access economic incentives to encourage sector information sharing and other desired behavior.

To facilitate private-sector participation, PDD 63 also encouraged the voluntary creation of information sharing and analysis centers (ISACs) to serve as mechanisms for gathering, analyzing, and appropriately sanitizing and disseminating information to and from infrastructure sectors and the federal government through NIPC. PDD 63 also suggested several key ISAC activities to effectively gather, analyze, and disseminate information—activities that could improve the security postures of the individual sectors and provide an improved level of communication within and across sectors and all levels of government. These activities are: establishing baseline statistics and patterns on the various infrastructures; serving as a clearinghouse for information within and among the various sectors; providing a library of historical data for use by the private-sector and government, and reporting private-sector incidents to NIPC.

The Homeland Security Act of 2002 Established the Department's CIP Responsibilities

The Homeland Security The Homeland Security Act of 2002, signed by the President on November 25, 2002, established DHS. To help accomplish its mission, the act Act of 2002 Established the established five under secretaries, among other entities, with responsibility over directorates for management, science and technology, information analysis and infrastructure protection, border and transportation security, and emergency preparedness and response.

The act made the Information Analysis and Infrastructure Protection (IAIP) Directorate within the department responsible for CIP functions and transferred to it the functions, personnel, assets, and liabilities of several existing organizations with CIP responsibilities, including NIPC (other than the Computer Investigations and Operations Section).

IAIP is responsible for accessing, receiving, and analyzing law enforcement information, intelligence information, and other threat and incident information from respective agencies of federal, state, and local governments and the private-sector, and for combining and analyzing such information to identify and assess the nature and scope of terrorist threats. IAIP is also tasked with coordinating with other federal agencies to administer the Homeland Security Advisory System to provide specific warning information along with advice on appropriate protective measures and countermeasures. Further, IAIP is responsible for disseminating, as appropriate, information analyzed by DHS within the department, to other federal agencies, to state and local government agencies, and to private-sector entities.

Moreover, as stated in the Homeland Security Act of 2002, IAIP is responsible for (1) developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States and (2) recommending measures to protect the key resources and critical infrastructure of the United States in coordination with other federal agencies and in cooperation with state and local government agencies and authorities, the private-sector, and other entities.

National Strategies Establish Information-Sharing Initiatives

The *National Strategy for Homeland Security* identifies information sharing and systems as one foundation for evaluating homeland security investments across the federal government. It also identifies initiatives to enable critical infrastructure information sharing and to integrate sharing across state and local government, private industry, and citizens. Consistent with the original intent of PDD 63, the *National Strategy for Homeland Security* states that, in many cases, sufficient incentives exist in the private market for addressing the problems of CIP. However, the strategy also discusses the need to use all available policy tools to protect the health, safety, or well-being of the American people. It mentions federal grant programs to assist state and local efforts, legislation to create incentives for the private sector, and, in some cases, regulation.

The *National Strategy to Secure Cyberspace* provides an initial framework for both organizing and prioritizing efforts to protect our nation's cyberspace. It also provides direction to federal departments and agencies that have roles in cyberspace security and identifies steps that state and local governments, private companies and organizations, and individual Americans can take to improve our collective cybersecurity. The strategy warns that the nation's private-sector networks are increasingly targeted and will likely be the first organizations to detect attacks with potential national significance. According to the cyberspace strategy, ISACs, which possess unique operational insight into their industries' core functions and will help provide the necessary analysis to support national efforts, are expected to play an increasingly important role in the National Cyberspace Security Response System[2] and the overall missions of homeland security. In addition, the cyberspace strategy identifies DHS as the central coordinator for cyberspace efforts and requires it to work closely with the ISACs to ensure that they receive timely and threat and vulnerability data that can be acted on and to coordinate voluntary contingency planning efforts. The strategy reemphasizes that the federal government encourages the private-sector to continue to establish ISACs and, further, to enhance the analytical capabilities of existing ISACs. Moreover, the strategy stresses the need to improve and enhance public-private information sharing about cyber attacks, threats, and vulnerabilities and to encourage broader information sharing on cybersecurity among nongovernmental organizations with significant computing resources. The *National Strategy to Secure Cyberspace* also states that the market is to provide the majorimpetus to improve cybersecurity and that regulation will not become a primary means of securing cyberspace.

The *National Strategy for the Physical Protection of Critical infrastructures and Key Assets* provides a statement of national policy to remain committed to protecting critical infrastructures and key assets from physical attacks. It outlines three key objectives to focus the national protection effort: (1) identifying and assuring the protection of the most critical assets, systems, and functions; (2) assuring the protection of infrastructures that face an imminent threat; and (3) pursuing collaborative measures and initiatives to assure the protection of other potential targets. The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* also states that further government leadership and intense collaboration between public—and private-sector stakeholders is needed to create a more effective and efficient information-sharing process to enable our core protective missions. Some of the specific initiatives include

- defining protection-related information requirements and establishing effective, efficient information-sharing processes;
- promoting the development and operation of critical sector ISACs, including developing advanced analytical capabilities;
- improving processes for domestic threat data collection, analysis, and dissemination to state and local governments and private industry; and
- completing implementation of the Homeland Security Advisory System.

The *National Strategy for the Protection of Critical Infrastructures and Key Assets* reiterates that additional regulatory directives and mandates should only be necessary in instances where the market forces are insufficient to prompt the necessary investments to protect critical infrastructures and key assets.

Current Federal Agency CIP Responsibilities

[2] The National Cyberspace Security Response System is a public-private architecture, coordinated by the Department of Homeland Security, for analyzing and warning; managing incidents of national significance; promoting continuity in government systems and private sector infrastructures; and increasing information sharing across and between organizations to improve cyberspace security. It includes governmental entities and nongovernmental entities, such as private-sector ISACs.

In December 2003, the President issued HSPD–7, which established a national policy for federal departments and agencies to identify and prioritize critical infrastructure and key resources and to protect them from terrorist attack. It superseded PDD 63. HSPD–7 defines responsibilities for DHS, lead federal agencies, or sector-specific agencies that are responsible for addressing specific critical infrastructure sectors,and other departments and agencies. It instructs federal departments and agencies to identify, prioritize, and coordinate the protection of critical infrastructure to prevent, deter, and mitigate the effects of attacks.

The Secretary of Homeland Security is assigned several responsibilities, including

- coordinating the national effort to enhance critical infrastructure protection;
- identifying, prioritizing, and coordinating the protection of critical infrastructure, emphasizing protection against catastrophic health effects or mass casualties;
- establishing uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across sectors; and
- serving as the focal point for cyberspace security activities, including analysis, warning, information sharing, vulnerability reduction, mitigation, and recovery efforts for critical infrastructure information systems.

To ensure the coverage of critical sectors, HSPD–7 designated sector specific agencies, formerly referred to as lead agencies, for the critical infrastructure sectors identified in the *National Strategy for Homeland Security* (see table 1). These agencies are responsible for infrastructure protection activities in their assigned sectors, which include

- coordinating and collaborating with relevant federal agencies, state and local governments, and the private-sector to carry out their responsibilities;
- conducting or facilitating vulnerability assessments of the sector;
- encouraging the use of risk management strategies to protect against and mitigate the effects of attacks against the critical infrastructure.
- identifying, prioritizing, and coordinating the protection of critical infrastructure;
- facilitating the sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices; and
- reporting to DHS on an annual basis on their activities to meet these responsibilities.

Further, the sector-specific agencies are to continue to encourage the development of information-sharing and analysis mechanisms and to support sector-coordinating mechanisms. HSPD–7 does not suggest any specific ISAC activities.

Table 1: Critical Infrastructure Sectors Identified by the National Strategy for Homeland Security and HSPD–7

Sector	Description	Sector-specific agency
Agriculture	Provides for the fundamental need for food. The infrastructure includes supply chains for feed and crop production.	Department of Agriculture
Banking and Finance	Provides the financial infrastructure of the nation. This sector consists of commercial banks, insurance companies, mutual funds, government sponsored enterprises, pension funds, and other financial institutions that carry out transactions including clearing and settlement.	Department of the Treasury
Chemicals and hazardous materials	Transforms natural raw materials into commonly used products benefiting Department of Homeland society's health, safety, and productivity. The chemical industry Security represents a $450 billion enterprise and produces more than 70,000 products that are essential to automobiles, pharmaceuticals, food supply, electronics, water treatment, health, construction and other necessities.	Department of Homeland Security

Table 1: Critical Infrastructure Sectors Identified by the National Strategy for Homeland Security and HSPD–7—Continued

Sector	Description	Sector-specific agency
Defense industrial base	Supplies the military with the means to protect the nation by producing weapons, aircraft, and ships and providing essential services, including information technology and supply and maintenance.	Department of Defense
Emergency services	Saves lives and property from accidents and disaster. This sector includes fire, rescue, emergency medical services, and law enforcement organizations.	Department of Homeland Security
Energy	Provides the electric power used by all sectors, including critical infrastructures, and the refining, storage, and distribution of oil and gas. The sector is divided into electricity and oil and natural gas.	Department of Energy
Food	Carries out the post-harvesting of the food supply, including processing and retail sales.	Department of Agriculture and Department of Health and Human Services
Government	Ensures national security and freedom and administers key public functions.	Department of Homeland Security
Information technology and telecommunications	Provides communications and processes to meet the needs of businesses and government.	Department of Homeland Security
Postal and shipping	Delivers private and commercial letters, packages, and bulk assets. The U.S. Postal Service and other carriers provide the services of this sector.	Department of Homeland Security
Public Health and Healthcare	Mitigates the risk of disasters and attacks and also provides recovery assistance if an attack occurs. The sector consists of health departments, clinics, and hospitals.	Department of Health and Human Services
Transportation	Enables movement of people and assets that are vital to our economy, mobility, and security with the use of aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit.	Department of Homeland Security
Drinking water and water treatment systems	Sanitizes the water supply with the use of about 170,000 public water systems. These systems depend on reservoirs, dams, wells, treatment facilities, pumping stations, and transmission lines.	Environmental Protection Agency

Source: GAO analysis based on the President's National Strategy documents and HSPD–7.

In January, the President issued HSPD–9, which established a national policy to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies. HSPD–9 defines responsibilities for DHS, lead federal agencies, or sector-specific agencies, responsible for addressing specific critical infrastructure sectors, and other departments and agencies. It instructs federal departments and agencies to protect the agriculture and food system from terrorist attacks, major disasters, and other emergencies by

- identifying and prioritizing sector-critical infrastructure and key resources for establishing protection requirements;
- developing awareness and early warning capabilities to recognize threats;
- mitigating vulnerabilities at critical production and processing nodes;
- enhancing screening procedures for domestic and imported products; and

In addition, the Secretary of Homeland Security, in coordination with the Secretaries of Agriculture, Health and Human Services, and other appropriate federal department and agencies, are assigned responsibilities including:

- expanding and continuing vulnerability assessments of the agriculture and food sectors; and
- working with appropriate private-sector entities to establish an effective information-sharing and analysis mechanism for agriculture and food.
- enhancing response and recovery procedures.

Prior GAO Recommendations

We have made numerous recommendations over the last several years related to information-sharing functions that have been transferred to DHS. One significant area of our work concerns the federal government's CIP efforts, which is focused on sharing information on incidents, threats, and vulnerabilities and providing warnings related to critical infrastructures both within the federal government and between the federal government and state and local governments and the private sector. Although improvements have been made in protecting our nation's critical infrastructures and continuing efforts are in progress, further efforts are needed to address the following critical CIP challenges that we have identified:

- developing a comprehensive and coordinated national plan to facilitate CIP information sharing, which clearly delineates the roles and responsibilities of federal and nonfederal CIP entities, defines interim objectives and milestones, sets timeframes for achieving objectives, and establishes performance measures;
- developing fully productive information-sharing relationships within the federal government and between the federal government and state and local governments and the private-sector;
- improving the federal government's capabilities to analyze incident, threat, and vulnerability information obtained from numerous sources and share appropriate timely, useful warnings and other information concerning both cyber and physical threats to federal entities, state and local governments, and the private-sector; and
- providing appropriate incentives for nonfederal entities to increase information sharing with the federal government.

ISAC Structures and Operations Reflect Sector Needs and Evolving Goals

PDD 63 encouraged the voluntary creation of ISACs and suggested some possible activities, as discussed earlier; however, their actual design and functions were left to the private-sector, along with their relationship with the federal government. HSPD–7 continues to encourage the development of information-sharing mechanisms and does not suggest specific ISAC activities. As a result, the ISACs have been designed to perform their missions based on the unique characteristics and needs of their individual sectors and, although their overall missions are similar, they have different characteristics. They were created to provide an information-sharing and analysis capability for members of their respective infrastructure sectors to support efforts to mitigate risk and provide effective response to adverse events, including cyber, physical, and natural events. In addition, the ISACs have taken several steps to improve their capabilities and the services they provide to their respective sectors.

Management and Operational Structures Vary, But Provide Similar Basic Capabilities

The ISACs have developed diverse management structures and operations to meet the requirements of their respective critical infrastructure sectors. To fulfill their missions, they have been established using various business models, diverse funding mechanisms, and multiple communication methods.

Business model—ISACs use different business models to accomplish their missions. Most are managed or operated as private entities, including the Financial Services, Chemical, Electricity Sector, Food, Information Technology, Public Transit, Real Estate, Surface Transportation, Highway, and Water ISACs. Many are established as part of an association that represents a segment of or an entire critical infrastructure sector. For example, the Association of Metropolitan Water Authorities manages the contract for the Water ISAC and the American Chemistry Council manages and operates the Chemical ISAC through its CHEMTRAC.[3] In addition, the North American Electric Reliability Council (NERC),[4] a nonprofit corporation

[3] The American Chemistry Council represents the leading companies engaged in the business of chemistry. CHEMTREC® (Chemical Transportation Emergency Center) is the American Chemistry Council's 24-hour emergency communications center. It was established in 1971 to provide emergency responders technical assistance in safely mitigating a distribution incident.

[4] The North American Electric Reliability Council's (NERC) membership includes small and large electric utilities, regional utility companies, power marketers, and other entities responsible for power generation, transmission, control, and marketing and distribution in the United States, Canada, and a portion of Mexico.

that promotes electric system reliability and security, operates the Electricity Sector ISAC using internal expertise.

The legal structure of ISACs continues to evolve. The Financial Services ISAC has evolved from a limited liability corporation in 1999 to a 501(c)6 non-stock corporation and is managed by a board of directors that is comprised of representatives from the Financial Services ISAC's members. According to the Financial Services ISAC Board, the change to be a 501(c)6 non-stock corporation, as mentioned above, was made to simplify the membership agreement and to make the process for obtaining public funding easier. The Energy ISAC also changed from a limited liability corporation to a 501(c)3 nonprofit charitable organization to eliminate membership barriers.

Also, government agencies have partnered with the private-sector to operate certain ISACs. For example, DHS's National Communications Systems/ National Coordinating Center (NCC) for Telecommunications sponsors the Telecommunications ISAC, which is a government/industry operational and collaborative body.[5] DHS provides for the Telecommunications ISAC facilities, tools and systems, the NCC manager, and the 24x7 watch operations staff. The private-sector provides representatives who have access to key corporate personnel and other resources. In addition, DHS's United States Fire Administration operates the Emergency Management and Response ISAC. New York State, through its Office of Cyber Security and Critical Infrastructure Coordination, is coordinating efforts of the Multi-state ISAC. The New York State Office of Cyber Security and Critical Infrastructure Coordination is currently studying best practices and lessons learned to assist in developing a structure that will include representation by member states.

Six of the ISACs included in our study use contractors to perform their day-to-day operations. According to an Association of Metropolitan Water Agencies (AMWA) official, they chose a contractor to operate the Water ISAC because the contractor had the appropriate expertise. In addition, the contractor's personnel had government clearances and the ability to operate a secure communication system and facility. In addition, ISACs use contractors to supplement their operations. For example, a formal contract provides for the daily staffing and performance of the Emergency Management and Response ISAC's tasks. It chose this model because of federal requirements and the shortage of positions for federal full-time employees at the United States Fire Administration. The Telecommunications ISAC contracted for analysts to operate the 24 x 7 watch operations under the management of a government official.

ISACs also differ in the nature of the hazards that they consider: cyber, physical, or all hazards (including natural events such as hurricanes). For example, during events of the power outage in August 2003 and Hurricane Isabel in September 2003, the Financial Services ISAC was contacted by DHS to determine the Banking and Finance sector's preparedness and the impact of those events. However, the Multi-state ISAC will remain focused on cyber threats because other state organizations are in place to address physical and natural disaster events.

Funding—ISACs fund their activities using a variety of methods—fees-for-service, association sponsorship, federal grants, and voluntary, or inkind, operations by existing participants. For example, the Financial Services, Information Technology, and Water ISACs use a tiered fee-for-service model for members. This model establishes different tiers of membership based on the level of service provided. These tiers typically include some basic level of service that is provided at minimal or no cost to the member and additional tiers that provide—for a fee—more personalized service and access to additional resources. To help ensure that cost is not a deterrent to membership and that the ISAC's coverage of its sector is extensive, the Financial Services ISAC recently, as part of its next-generation ISAC effort, shifted to a tiered fee-for-service approach. It offers five levels of service that vary in cost—Basic (no charge), Core ($750 per year), Premier ($10,000 per year), Gold ($25,000 per year), and Platinum ($50,000)—for ascending levels of information and analytical capabilities. In addition, there is a partner-level license agreement for select industry associations ($10,000) for distribution to eligible association members of Urgent and Crisis Alerts. For example, the Information Technology ISAC recently started to work on a tiered basis with fees set annually at $40,000; $25,000; $5,000;

[5] The National Coordinating Center for Telecommunications is open to companies that provide telecommunications or network services, equipment, or software to the communications and information sector; select, competitive local exchange carriers; Internet service providers; vendors; software providers; telecommunications professional organizations and associations; or companies with participation or presence in the communications and information sector. Membership is also allowed for National Coordinating Center member federal departments and agencies, and for national security/emergency preparedness users.

$1,000; and free. The Water ISAC also uses a tiered approach, with membership fees ranging from $7,500 to $750 annually. The Surface Transportation ISAC assesses an annual fee from its Class I railroad members of approximately $7,500.

Some industry associations that operate ISACs fund them from budgets. For example, the North American Electric Reliability Council (NERC) funds the Electricity Sector ISAC, and the American Trucking Association funds the Highway ISAC from their budgets. The American Chemistry Council fully funds the Chemical ISAC through the previously existing Chemical Transportation Emergency Center, known as CHEMTRAC. The ten trade associations that are members of it fund the Real Estate ISAC.

In addition, some ISACs receive funding from the federal government for such purposes as helping to start operations, funding memberships, and providing expanded capabilities. Examples include the following:

- The Public Transit ISAC initially received a $1.2 million grant from the Federal Transit Administration (FTA) to begin operations. Members pay no an annual fee and there are no membership requirements from the association that started the ISAC—the American Public Transportation Association.
- For FY 2004, the Water ISAC received a $2 million grant from EPA to cover annual operating costs, including the expansion of memberships to smaller utilities.
- The Financial Services ISAC received $2 million dollars from the Department of the Treasury to enhance its capabilities, including technology to broaden membership service.
- The Highway ISAC received initial funding from DHS's Transportation Security Administration (TSA) to start the ISAC.
- The Energy ISAC received federal grants to assist entities within its separate sectors to be members.
- DHS provides funding for the operation of the Telecommunications ISAC that is combined with in-kind services provided by the corporate participants. DHS also fully operates the Emergency Management and Response ISAC.

States also provide funding for ISACs. For example, the Multi-state ISAC is funded by and functions as part of the New York State Cyber Security Analysis Center. In addition, the Research and Education Network ISAC is supported by Indiana University.

Sharing mechanisms—ISACs use various methods to share information with their members, other ISACs, and the federal government. For example, they generally provide their members access to electronic information via e-mail and Web sites. For example, the Chemical ISAC members receive e-mail alerts and warnings in addition to the information that is posted to the ISAC's Web site. The Highway ISAC provides members on its Web site with links to IT resources.

Some ISACs also provide secure members-only access to information on their Web sites. For example, the Financial Services ISAC's Web site offers multiple capabilities for members at the premier level and above, including, among other things, access news, white papers, best practices, and contacts. The Energy ISAC offers its members access to a secure Web site.

In addition, some ISACs hold conference calls for their members. For example, the Chemical ISAC holds biweekly conference calls with DHS. The Financial Services ISAC also conducts threat intelligence conference calls every two weeks for premier members and above with input from Science Applications International Corporation (SAIC) and DHS. These calls discuss physical and cyber threats, vulnerabilities and incidents that have occurred during the previous two weeks, and they provide suggestions on what may be coming. The Financial Services ISAC is capable of organizing crisis conference calls within an hour of the notification of a Crisis Alert, and it hosts regular bi-weekly threat conference calls for remediation of vulnerabilities (viruses, patches).

ISACs also use other methods to communicate. For example, they may use pagers, phone calls, and faxes to disseminate information. In addition, the Telecommunications ISAC uses the Critical Infrastructure Warning Information Network (CWIN).[6] The Financial Services ISAC also sponsors twice yearly members' only conferences to learn and share information.

ISAC Coverage and Participation Varies

According to the ISAC Council, its membership possesses an outreach and connectivity capability to approximately 65 percent of the U.S. private critical infra-

[6] CWIN provides connectivity and 24x7 alert and notification capability to government and industry participants. It is engineered to provide a reliable and survivable network capability, and it has no logical dependency on the Internet or the Public Switched Network.

structure. However, the ISACs use various matrices to define their respective sectors' participation in their activities. For example, the Banking and Finance sector has estimated that there are more than 25,000 financial services firms in the United States. Of those, according to the Financial Services ISAC Board, roughly 33 percent receive Urgent and Crisis Alerts through license agreements with sector associations—accounting for the vast majority of total commercial bank assets, the majority of assets under management, and the majority of securities/ investment bank transactions that are handled by the sector, but less than half the sector's insurance assets. According to an American Public Transportation Association official, the Public Transit ISAC covers a little less than 5 percent of the public transit agencies; however, those agencies handle about 60 to 70 percent of the total public transit ridership. Further, according to NERC officials, virtually all members of NERC are members of the Electricity Sector ISAC. As for the Energy ISAC, officials stated that its 80-plus members represent approximately 85 percent of the energy industry. Membership in the Information Technology ISAC also represents 85 to 90 percent of the industry, including assets of Internet equipment hardware, software, and security providers. For other ISACs, such as Chemical and Real Estate, officials stated that it is difficult to determine the percentage of the sector that is included.

Table 2 provides a summary of the characteristics of the ISACs that we included in our review. In addition to these ISACs, the Healthcare sector is continuing to organize, including efforts to establish an ISAC. According to DHS officials, the Emergency Law Enforcement ISAC that was formally operated by the NIPC and transferred to IAIP is not currently staffed and will be considered in current efforts to organize the Emergency Services sector.

Table 2: Summary of ISAC Characteristics

Critical Infrastructures and their ISAC(s)	Coverage	Funding model	Hazards covered	Analysis capability	Sharing mechanisms
Agriculture **None at this time.**					
Banking & Finance					
Financial Services (est. Oct. 1999)	200 members, including commercial banks, securities firms, and insurance companies. Represents 90% of the financial sector's assets.	Funded by and operated with tiered membership fees. Contractor operated.	Cyber Physical	Operates 24 hours a day, 7 days a week. Watch desk analyzes and categorizes threats, incidents, and warnings based on the sector's needs.	Text-based alerts, through a notification system, backed up by telephone. Biweekly threat intelligence conference call with DHS and SAIC.
Chemicals & Hazardous Materials					
Chemical (est. April 2002)	538 individual members representing the chemical industries. 285 businesses. Represents 90% of chemical sector.	Funded and operated by ACC's Chemical Transportation Emergency Center.	Cyber Physical	Operates 24x7. Currently working to develop an analysis center.	E-mails alerts and warnings. Chemistry ISAC Web site. Biweekly conference calls with DHS. Secure communications network with DHS.
Defense Industrial Base **None at this time.**					
Emergency Services					
Emergency Management & Response (est. Oct. 2000)	10 FEMA Regions 6 major stakeholders of EMR sector. Represents 100% of the essential components of the EMR Sector.	Funded by FEMA's Office of Cyber Security with supplementation from USFA. Contractor operated.	Cyber Physical	Developing 24x7 operations. Analyzes and disseminates actionable intelligence on threats, attacks, vulnerabilities, anomalies, and security best practices.	Electronic messaging Telephone and when necessary, a secure telephone unit.
Energy					

Electric (est. Oct. 2000)	More then 90% of NERC members are members of the ISAC including large and small electric utilities, regional electric utility companies, and power marketers.	Funded and managed/operated by NERC.	Cyber Physical	Operates 24x7. The ES–ISAC and NERC have created the Indications, Analysis, and Warnings Program (IAW) that provides a set of guidelines for reporting operational and cyber incidents that adversely affect the electric power infrastructure.	Secure telephone, fax, and Web server E-mail Satellite telephones. Information such as incident reports and warnings, vulnerability assessments, and related documents are posted on the public Web site.
Energy (est. Nov. 2001)	80 plus members from the oil and gas sector. Represents 85% of the oil and gas sector.	Funded by grants from DOE. Contractor operated.	Cyber Physical	Operates 24x7. Analyzes threats, vulnerabilities, and incident information. Provides security information and solutions.	Conference calls Fax, Email, pager. Detailed information on warnings provided on a membership only, secure Web site.
Food					
Food (est. Feb. 2002)	Over 40 food-industry trade associations and their members.	No current funding. Operated by volunteer labor from each member association.	Physical	Operates 24x7. No analysis capability, due to members' privacy concerns. Depends on DHS for analysis.	E-mail Watch Commander List Currently working to develop a secure email system.
Government					
State Gov. (est. Jan. 2003)	49 states (excluding Kansas) and the District of Columbia.	Funded and operated by New York State. States provide time and resources as appropriate.	Cyber Physical & Natural (as it relates to cyber).	Operates 24x7. Issues bulletins, advisories, and alerts.	Monthly conference calls E-mail Telephone
Information Technology & Telecommunications					
IT (est. Dec. 2000)	90% of all desktop operating systems. 85% of all databases. 50% of all desktop computers. 85% of all routers. 65% of software security.	Funded and operated by foundational member contributions, will soon implement membership fees (tiered). Contractor operated.	Cyber Physical	Operates 24x7. Analyzes cyber alerts and advisories and reports physical issues.	CWIN Encrypted e-mail SSL-protected Web sites Cellular phones VoIP telephony GETS)[7] system for priority calls

Table 2: Summary of ISAC Characteristics—Continued

Critical Infrastructures and their ISAC(s)	Coverage	Funding model	Hazards covered	Analysis capability	Sharing mechanisms
Telecom (est. Jan. 2000)	95% of wireline providers. Over 60% of wireline vendors. 95% of wireless providers. 90% of wireless vendors. 42% of Internet Service subscribers. 90% of Internet Service networks. 6 of the top system integrators in the U.S. Federal IT market. 15% of Domain Name Service root and global Top Level Domain operators.	Funded by NCS. Operated by NCC. Agencies bear the costs of their own personnel.	Cyber Physical Natural	Operates 24x7. Analyzes data to avoid crises that could affect the entire telecom infrastructure.	E-mail Telephone Fax Meetings CWIN
Research & Education Network (est. Feb. 2003)	200 Universities. All U.S. universities and colleges that are connected to national R&E networks have basic membership.	Funded and operated by Indiana University.	Cyber	Operates 24x7. Receives and disseminates information regarding network security vulnerabilities and threats in the higher education community.	Public information restricted to aggregate views of the network. Information identifying institutions or individuals not reported publicly. Detailed and sensitive information shared only with affected institutions.
Postal & Shipping None at this time.					
Public Health & Healthcare					
HealthCare None at this time.					
Transportation					

Public Transit (est. Jan. 2003)	Approximately 100 of the major national transit organizations.	Federally funded. Contractor operated.	Cyber Physical	Operations 24x7. Collects, analyzes, and disseminates security information.	E-mail tree Secure e-mail Public Transit Web site Links to HSOC, and DOT and TSA's Operation Centers.
Surface Transportation (est. May 2002)	Includes the major North American freight railroads and Amtrak. Represents 95% of the U.S. freight railroad industry and Amtrak.	Funded by membership fees and a grant from the Federal Transit Administration (FTA). Contractor operated.	Cyber Physical Natural	Operates 24x7. Conducts mid— to longterm technical analysis on all threats.	Surface Transportation Web site. Secure telephone.
Highway (est. March 2003)	Over 90% of the largest for-hire motor carriers. Represents 60% economic activity with over 50% of long haul.	Funded and operated by the American Trucking Association (ATA).	Cyber Physical	Developing 24x7 operations. Channels warnings, threat information, and advisories to the industry and to drivers through its call center.	Highway ISAC Web site Highway watch center Blast fax E-mail Print media communications Amber alerts
Drinking Water & Water Treatment Systems					
Water (est. Dec. 2002)	275–300 small and large water utilities. Represents 45% of water utilities with secure portals. Represents 85% of the water utilities that receive e-mail alerts.	Funded by tired membership fees and a grant from EPA. Contractor operated. Receives contributions from AMWA.	Cyber Physical	Operates 24x7. Analyzes threat and incident information for its potential impact on the sector.	Encrypted e-mail Secure portal Secure electronic bulletin boards and chat rooms
Other Sectors That Have Established ISACs					
Real Estate (est. April 2003)	10 trade associations representing hotels, realtors, shopping centers, and others.	Funded by trade associations. Contractor operated.	Physical	Operates 24x7. Depends on DHS for threat analysis.	2-way communications network and Web site Conference calls with top executives from various sectors as needed.

[7] Government Emergency Telecommunications Service (GETS)

Sector Coordinator Roles Differ

As discussed earlier, federal CIP policy establishes the position of sector coordinator for identified critical infrastructure sectors to initiate and build cooperative relationships across an entire infrastructure sector. In most cases, sector coordinators have played an important role in the development of their respective infrastructure sectors' ISACs. In many cases the sector coordinator also manages or operates the ISAC.

- The North American Electric Reliability Council, as sector coordinator for the electricity segment of the energy sector, operates the Electricity Sector ISAC.
- The Association of American Railroads, as a sector coordinator for the transportation sector, manages the Surface Transportation ISAC.
- The Association of Metropolitan Water Agencies, as the sector coordinator for the water and wastewater sector, manages the Water ISAC

In addition, regarding the telecommunications ISAC, sector coordinators participate as members of the ISAC. For example, the Cellular Telecommunications and Internet Association, the United States Telecom Association, and the Telecommunications Industry Association are all members of the NCC, which operates the telecommunications ISAC. In the case of the Financial Services ISAC, no formal relationship exists between the Banking and Finance Sector Coordinator, the Financial Services Sector Coordinating Council, and the ISAC; however, according to Financial Services ISAC officials, there is a good relationship between them.

Other ISACs were created and are operated without a formal sector coordinator in place, including the Chemical, Emergency Management and Response, and Food ISACs.

Council Established to Improve ISACs' Efficiency and Effectiveness

Eleven ISACs created an ISAC Council to work on various operational, process, and other common issues to effectively analyze and disseminate information and, where possible, to leverage the work of the entire ISAC community. The ISACs initiated this effort without federal sponsorship. Currently, the participating ISACs include Chemical, Electricity, Energy, Financial Services, Information Technology, Public Transit, Surface Transportation, Telecommunications, Highway, and Water. In addition, the Multi-state and Research and Education Networks ISACs are participants.

In February 2004, the council issued eight white papers to reflect the collective analysis of its members and to cover a broad set of issues and challenges, including

- **Government/Private-sector Relations.** Explains the need for DHS to clarify its expectations and to develop roles and responsibilities for the ISACs.
- **HSPD–7 Issues and Metrics.** Describes specific issues related to the private-sector that DHS should address when responding to HSPD–7.
- **Information Sharing and Analysis.** Identifies future goals that the ISACs may want to work on achieving, including developing an implementation plan.
- **Integration of ISACs into Exercises.** Discusses the importance of the ISACs and the private infrastructure sectors being involved in government exercises that demonstrate responses to possible incidents.
- **ISAC Analytical Efforts.** Describes the various levels of capabilities that individual ISACs may want to consider supporting, including cyber and physical analysis.
- **Policy and Framework for the ISAC Community.** Identifies common policy areas that need to be addressed to provide effective, efficient, and scalable information sharing among ISACs and between ISACs and the federal government.
- **Reach of Major ISACs.** Describes and identifies the degree of outreach that the ISACs have achieved into the U.S. economy. As of September 2003, the ISAC Council estimated that the ISACs had reached approximately 65 percent of the critical infrastructures they represent.
- **Vetting and Trust.** Discusses the processes for sharing information and the need to develop trust relationships among individual ISAC members and among the various ISACs.

Federal Efforts to and Interaction with the ISACs Continue

As outlined in HSPD–7 and presented in table 1, DHS and other federal agencies are designated as sector-specific agencies for the critical Establish Cooperation infrastructure sectors identified. In addition, DHS is responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States and has established organizational structures to address its CIP and information-sharing responsibilities. DHS and the sector-specific agencies have undertaken a number of efforts to address the public/private partnership that is called for by federal CIP policy, and they continue to work on their cooperation and interaction with the ISACs and with each other.

DHS Actions to Improve Information-sharing Relationships

The functions DHS provides to each ISAC differ, and its coordination and levels of participation vary for each sector-specific agency. However, the department has undertaken a number of efforts with the ISACs and sector specific agencies to implement the public/private partnership called for by federal CIP policy.

DHS has established functions within the department to support the ISACs and other CIP efforts. IAIP, as the DHS component directly responsible for CIP activities, carries out many of these functions. The Infrastructure Coordination Division within IAIP plays a key role in coordinating with the ISACs concerning information sharing. Nonetheless, ISACs may interact with multiple components of the department. For example, the ISACs may discuss cyber issues with the National Cyber Security Division. According to a DHS official, the department does not intend to establish a single point of contact for ISACs within the department. Rather, the department plans to develop policies and procedures to ensure effective coordination and sharing of ISAC contact information among the appropriate DHS components. In addition, the Infrastructure Coordination Division is in the process of staffing analysts who are responsible for working with each critical infrastructure sector. The analysts would serve as the primary point of contact for the sectors and would address information sharing, coordination, information protection, and other issues raised by the sectors.

Further, according to DHS officials, TSA, within the department's Border and Transportation Security Directorate, is working with organizations in the private sector to establish information-sharing relationships. For example, Surface Transportation ISAC analysts stated that they have a good working relationship with TSA, and TSA's Operations Center has office space designated for them.

In addition, other DHS actions include the following:

- Last summer, DHS, the Department of Agriculture (USDA), and the Department of Health and Human Services' (HHS) Food and Drug Administration (FDA) initiated efforts to organize the agriculture and food critical infrastructure sectors to raise awareness and improve security efforts. An introductory conference was held with about 100 leading sector corporations and associations to make the business case for participating in CIP efforts, including the importance of enhancing security and sharing information within the sectors.
- In December, DHS hosted a 2-day CIP retreat with ISAC representatives, sector coordinators, and high-level DHS and White House Homeland Security Council officials. Participants discussed the needs, roles, and responsibilities of public—and private-sector entities related to information sharing and analysis, incident coordination and response activities, critical infrastructure information requests, and level of DHS funding. During this retreat, DHS participated in the first meeting of the Operational Clarity and Improvement Task Group, which was formed by the ISAC Council and sector coordinators to address the need for a common conceptual framework and to clarify current and future efforts to protect the nation's critical infrastructure.
- In January, DHS's IAIP Directorate held a 2-day conference to describe the information it is analyzing and the use of that information in the partnership with the private sector to discuss information sharing between the federal government and the private sector.
- In February, the department established the Protected Critical Infrastructure Information (PCII) Program, which enables the private sector to voluntarily submit infrastructure information to the government. DHS's IAIP Directorate is responsible for receiving submissions, determining if the information qualifies for protection and, if it is validated, sharing it with authorized entities for use as specified in the Critical Infrastructure Information Act of 2002.

In addition to the efforts listed above, DHS officials stated that they provide funding to some of the ISACs. For example, DHS has agreed to fund tabletop exercises for the Financial Services, Telecommunications, and Electricity Sector ISACs. DHS anticipates that the tabletop exercises will be completed by August 2004. Also, DHS expects to fund a cross-sector tabletop exercise. According to the Financial Services ISAC, funding for their tabletop exercise is $250,000.

Another effort that DHS has undertaken is to maintain regular contact with the ISACs. For example, a DHS analyst specializing in the chemical sector stated that the Chemical ISAC is in daily contact with DHS and that it participates in DHS-sponsored biweekly threat meetings. The department also conducts weekly conference calls with several ISACs, other DHS components, and private-sector organizations to discuss threats and viruses.

Sector-specific Agencies Have Taken Action to Assist the ISACs

HSPD–7 designates federal departments and agencies to be sector-specific agencies. These federal agencies, among other things, are to collaborate with the private sector and continue to encourage the development of information-sharing and analysis mechanisms. In addition, sector-specific agencies are to facilitate the sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices. Another directive, HSPD–9, establishes a national policy to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies. Some sector-specific agencies have taken steps to help the ISACs to increase their memberships and breadth of impact within their respective sectors and to improve their analytical and communications capabilities.

- **Environmental Protection Agency (EPA).** As noted earlier, EPA is the sector-specific agency for the water sector. According to EPA officials, its Office of Water (Water Security Division), which has been designated as the lead for drinking water and wastewater CIP efforts, is currently revising EPA's Office of Homeland Security's Strategic Plan. In addition, the division is working on a General Strategic Plan, to identify measurable goals and objectives and determine how the division will accomplish that work. Further, these officials stated that for fiscal year 2004, EPA issued a $2 million grant to the Water ISAC to enhance its capabilities, for example, to fund 24x7 operations and to increase and support ISAC membership. They also stated that EPA issued $50 million in grants to assist the largest drinking water utilities in conducting vulnerability assessments. There are also state grants to build communications networks for disseminating information, particularly to smaller utility companies. EPA's Water Security Division also makes publicly available various resources related to water security including, among other things, emergency response guidelines, risk assessment and vulnerability assessment methodologies, and a security product guide. The division has also developed a "Vulnerability Assessment Factsheet" that gives utility companies additional guidance on vulnerability assessments. Moreover, the Water Security Division holds biweekly conference calls with water associations to promote communications between EPA and the private sector, and it provides EPA publications and other information to the Water ISAC through e-mail distribution lists. In addition, the division has 10 regional offices that work with the states.
- **Department of the Treasury (Treasury).** As the sector-specific agency for the Banking and Finance sector, Treasury's Office of CIP and Compliance Policy is responsible for CIP-related efforts. It has developed policy for its role as a sector-specific agency. The policy includes steps to identify vulnerabilities with the assistance of the institutions, identify actions for remediation, and evaluate progress in reducing vulnerabilities. A major effort by Treasury was having consultants work with the Financial Services ISAC's board of directors to evaluate ways to improve the overall reach and operations of the ISAC. According to Treasury officials, this effort, in part, led to a $2 million grant from Treasury to the ISAC for developing the "next generation" Financial Services ISAC. The one-time grant was earmarked for enhancing the ISAC's capabilities. Regarding interaction with the Financial Services ISAC, Treasury informally shares high-level threat and incident information with the sector through the ISAC. The department also chairs the Financial and Banking Information Infrastructure Committee (FBIIC), a group of regulators who coordinate regulatory efforts to improve the reliability and security of financial systems. This group has done a number of things to raise awareness and improve the reliability of the institutions. For example, under the sponsorship of the Federal Deposit Insurance Corporation, there are regional outreach briefings that address why the private sector needs to partner with the federal government to improve its security. Moreover, FBIIC has sponsored the 3,600 priority telecommunications circuits for financial institutions under the National Communications System's Telecommunications Service Priority and Government Emergency Telecommunications Service programs.
- **Department of Energy (DOE).** As the sector-specific agency for the Energy and Electricity sectors, DOE's Office of Energy Assurance is responsible for fulfilling the roles of critical infrastructure identification, prioritization, and protection for the energy sector, which includes the production, refining, and distribution of oil and gas, and electric power—except for commercial nuclear power facilities. However, DOE does not address situational threats such as natural disasters or power outages with its ISACs because, in part, the ISACs are determining whether it is their role to address these types of threats. Information sharing with the ISACs is an informal process, and no written policy

exists. For example, DOE is collecting threat information related to hackers and computer security, but the department is not disseminating it to the ISACs or to private industry. The Office of Energy Assurance hopes to clarify and expand on this subject in its International Program Plan, which is currently in draft form.

- **Department of Health and Human Services (HHS).** As mentioned earlier, HHS is the sector-specific agency for the public health and healthcare sector, and it shares that role with USDA for the food sector. Currently, there is no ISAC for the healthcare sector. Efforts to organize the healthcare sector have been ongoing. In July 2002, HHS officials and other government and industry participants were invited to the White House conference center to discuss how they wanted to organize the sector. A Healthcare Sector Coordinating Council (HSCC) was formed, and HHS requested that MITRE, its contractor, lend technical support to the new group as it continues to organize the sector and establish an ISAC. In addition, HHS officials stated that the department provided $500,000 for ISAC efforts in fiscal year 2003 and budgeted $1 million for fiscal year 2004. HHS officials stated that the department would likely be agreeable to continuing to provide funding for an ISAC. They also stated that an ISAC could be operational within the next year. In the meantime, HHS is sharing information with the industry through an e-Community group that MITRE has set up on a secure Web site.

Agriculture and Food were only recently designated as critical infrastructure sectors and, as with the healthcare sector, efforts to organize the sectors are in the beginning stages. HHS has worked with the Food Marketing Institute-operated Food ISAC since it was established, but the department has focused more of its efforts on organizing the agriculture and food sectors. As we mentioned earlier, HHS helped initiate efforts to organize the sector by holding an introductory conference last summer for about 100 leading sector corporations and associations to make the business case for participating in CIP efforts. Recently, the department co-hosted a meeting with DHS and USDA in which industry participants were asked how they wished to organize into an infrastructure sector, including addressing the existence and expansion of the current Food ISAC. As a result of this meeting, participants agreed to establish a council of about 10–15 private-sector food and agriculture organizations to represent the sector. A federal government council will be created to interact with the private sector and with state and local governments. The government council will initially include several federal government agencies and state and local entities. According to HHS officials, the timeframe for organizing the sector and setting up an expanded Food ISAC has not been determined, but officials anticipated this occurring by fall of 2004.

- **Department of Agriculture (USDA).** As mentioned above, USDA shares with HHS the sector-specific agency designation for the food sector. USDA participated in a conference held last summer and a recent meeting with the industry. In addition to those events, USDA's Homeland Security Council Working Group is involved in enhancing the agriculture sector's information-sharing and analysis efforts, which may include replacing or improving the current Food ISAC. Another USDA effort uses training to reach out to the industry and raise awareness. For example, USDA is providing training to private-sector veterinarians and animal hospitals on recognizing possible signs of bioterrorism activity.

Although no longer a sector-specific agency for the transportation sector, DOT, through its Federal Transit Administration, has provided a grant to the Public Transportation ISAC to provide for memberships at no cost.

Challenges to ISAC Establishment and Partnership with the Federal Government

Increasing Sector Participation and Reach

Our discussions with the ISACs and the series of ISAC Council white papers confirmed that a number of challenges remain to the successful establishment and operation of ISACs and their partnership with DHS and other federal agencies. Highlighted below are some of the more significant challenges identified, along with any successful ISAC practices and related actions that have been taken or planned by DHS or others.

Many of the ISACs report that they represent significant percentages of their industry sectors; at least one—the Electricity ISAC—reports participation approaching 100 percent. The ISAC Council estimates that the overall ISAC community possess an outreach and connectivity capability to reach approximately 65 percent of the private critical infrastructure. The Council also recognizes the challenge of increasing sector participation, particularly to reach smaller entities that need security support, but have insufficient resources to actively contribute and pay for such support. Officials in DHS's IAIP acknowledge the importance of reaching out to critical infrastructure entities, and are considering alternatives to address this issue.

The Financial Services ISAC provides a notable example of efforts to respond to this challenge. Specifically, officials for this organization reported that, as of March 2003, its members represented a large portion of the sector's assets, but only 0.2 percent of the number of entities with small financial services firms and insurance companies, in particular, were underrepresented. To increase its industry membership, this organization established its next generation ISAC, which provides different levels of service—ranging from a free level of basic service to fees for value-added services—to help ensure that no entity is excluded because of cost. Further, it has set goals of delivering urgent and crisis alerts to 80 percent of the Banking and Finance sector by the end of 2004 and to 99 percent of the sector by the end of 2005. To help achieve these goals, the Financial Services ISAC has several other initiatives under way, including obtaining the commitment of the Financial Services Sector Coordinating Council (FSSCC—the sector coordinator and primary marketing arm for this ISAC) to drive the marketing campaign to sign up its members for the appropriate tier of service; encourage membership through outreach programs sponsored by the Federal Deposit Insurance Corporation and the FSSCC in 24 cities; and to work with individual sector regulators to include in their audit checklists whether a firm is a member of the ISAC. The Financial Services ISAC believes that its goals are attainable and points to its industry coverage, which it says had already increased to 30 percent in March 2004—only three months after its new membership approach began in December 2003.

Other issues identified that were related to increasing sector participation and reach included the following,

- Officials at two of the ISACs we contacted considered it important that the federal government voice its support for the ISACs as the principal tool for communicating threats.
- The ISAC Council has suggested that a General Business ISAC may need to be established to provide baseline security information to those general businesses that are not currently supported by an ISAC.
- Many of the industries that comprise our nation's critical infrastructures are international in scope. Events that happen to a private infrastructure or public sector organization in another country can have a direct effect in the United States, just as events here could have effects in other countries. Therefore, an ISAC may need to increase its reach to include the reporting and trust of international companies and organizations.

Building Trusted Relationships

A key element in both establishing an ISAC and developing an effective public/private partnership for CIP is to build trusted relationships and Building Trusted Relationships processes. From the ISAC perspective, sharing information requires a trusted relationship between the ISAC and its membership, such that companies and organizations know their sensitive data is protected from others, including competitors and regulatory agencies. According to the ISAC Council, the ISACs believe that they provide a trusted informationsharing and analysis mechanism for private industry in that they manage, scrutinize, establish, and authenticate the identity and ensure the security of their membership, as well as ensuring the security of their own data and processes. Other steps taken by ISACs to safeguard private companies' information, which may help to foster trusted relationships, included sharing information with other entities only when given permission to do so by the reporting entity and providing other protections, such as distributing sensitive information to subscribers through encrypted e-mail and a secure Web portal.

Building trusted relationships between government agencies and the ISACs is also important to facilitating information sharing. In some cases, establishing such relationships may be difficult because sector-specific agencies may also have a regulatory role; for example, the Environmental Protection Agency has such a role for the Water sector and HHS' Food and Drug Administration has it for portions of the Food and Agriculture sectors.

Information Sharing Between the Private Sector and Government

Sharing information between the federal government and the private sector on incidents, threats, and vulnerabilities continues to be a challenge. As we reported last year, much of the reluctance by ISACs to share information has focused on concerns over potential government release of that information under the Freedom of Information Act, antitrust issues resulting from information sharing within an industry, and liability for the entity that discloses the information.[8] However, our recent discussions with the ISACs—as well as the consensus of the ISAC Council—identified additional factors that may affect information sharing by both the ISACs and the government.

The ISACs we contacted all described efforts to work with their sector specific agencies, as well as with other federal agencies, ISACs, and organizations. For example, the Public Transit ISAC said that it provides a critical link between the transit industry, DOT, TSA, DHS, and other ISACs for critical infrastructures and that it collects, analyzes, and distributes cyber and physical threat information from a variety of sources, including law enforcement, government operations centers, the intelligence community, the U.S. military, academia, IT vendors, the International Computer Emergency Response Community, and others. Most ISACs reported that they believed they were providing appropriate information to the government but, while noting improvements, still had concerns with the information being provided to them by DHS and/or their sector specific agencies. These concerns included the limited quantity of information and the need for more specific, timely, and actionable information. In particular, one ISAC noted that it receives information from DHS simultaneously with or even after news reports, and that sometimes the news reports provide more details.

In its recent white papers, the ISAC Council also has identified a number of barriers to information sharing between the private sector and government. These included the sensitivity of the information (such as law enforcement information), legal limits on disclosure (such as Privacy Act limitations on disclosure of personally identifiable information), and contractual and business limits on how and when information is disclosed (e.g., the Financial Services ISAC does not allow any governmental or law enforcement access to its database). But the Council also emphasized that perhaps the greatest barriers to information sharing stem from practical and business considerations in that, although important, the benefits of sharing information are often difficult to discern, while the risks and costs of sharing are direct and foreseeable. Thus, to make information sharing real, it is essential to lower the practical risks of sharing information through both technical means and policies, and to develop internal systems that are capable of supporting operational requirements without interfering with core business. Consequently, the technical means used must be simple, inexpensive, secure, and easily built into business processes.

According to the Council, the policy framework must reduce perceived risks and build trust among participants. Further, the Council identified three general areas that must be addressed in policy for the information-sharing network to assure network participants that there is good reason to participate and that their information will be dealt with appropriately. These areas concern policies related to what information is shared within ISACs, across ISACs, and to and from government; actions to be performed at each node in the information-sharing network, including the kinds of analysis to be performed; and the protection of shared information and analysis in terms of both limitations on disclosure and use and information security controls.

The white papers also described the processes that are believed to be needed to ensure that critical infrastructure and/or security information is made available to the appropriate people with reasonable assurance that it cannot be used for malicious purposes or indiscriminately re-distributed so as to become essentially public information. These processes and other information-sharing considerations and tasks identified by the Council included the following:

- The ISAC information-sharing process needs to recognize two types of information categories—classified and sensitive but unclassified. However, the majority of information sharing must focus on the unclassified "actionable element" that points the recipient to a problem and to remediation action.
- Each ISAC is responsible for initially validating the trust relationship with its member organizations and for periodically re-assessing that trust relationship. The security structure must understand and continually be in dialogue with its vetted members and must manage this trusted relationship.
- Each individual who receives shared information must have a background check completed by and at a level of comprehensiveness specified by the sponsoring organization.

[8] U.S. General Accounting Office, *Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats,* GAO–03–173 (Washington, D.C.: Jan. 30, 2003); and *Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors,* GAO–03–233 (Washington, D.C.: Feb. 28, 2003).

- Consequences and remediation must be developed and understood to address situations in which information is disclosed improperly—either intentionally or unintentionally.
- The government's data and information requirements for the sectors and the sectors' requirements for the government need to be defined.
- The government should establish a standing and formal trusted information-sharing and analysis process with the ISACs and sector coordinators as the trusted nodes for this dissemination. This body should be brought in at the beginning of any effort, and DHS products should be released to this group for primary and priority dissemination to their respective sectors.

Building this trusted information-sharing and analysis process is also dependent on the protections the government provides for the sensitive data shared by ISACs and private companies. As discussed earlier, DHS recently issued the interim rule for submitting protected critical infrastructure information, which provides restrictions on the use of this information and exempts it from release under the Freedom of Information Act. However, it remains to be seen whether these protections will encourage greater private-sector trust and information sharing with the federal government.

Identifying Roles and Responsibilities

Federal CIP law and policies, including the Homeland Security Act of 2002, the *National Strategy to Secure Cyberspace,* and HSPD–7, establish CIP responsibilities for federal agencies, including DHS and others identified as sector-specific agencies for the critical infrastructure sectors. However, the ISACs believe that the roles of the various government and private sector entities involved in protecting critical infrastructures must continue to be identified and defined. In particular, officials for several ISACs wanted a better definition of the role of DHS with respect to them. Further, officials for two ISACs thought other agencies might more appropriately be their sector-specific agencies. Specifically, the Energy ISAC would like its sector-specific agency to be DHS and not the Department of Energy, which is also the regulatory agency for this sector. On the other hand, the Highway ISAC thought its sector-specific agency should be the Department of Transportation—the regulatory agency for its sector—and not DHS.

The ISAC Council also identified the need for DHS to establish the goals of its directorates and the relationships of these directorates with the private sector. The Council also wants clarification of the roles of other federal agencies, state agencies, and other entities—such as the National Infrastructure Assurance Council.

Obtaining Government

Ten of the ISACs we contacted, plus the Healthcare sector, emphasized the importance of government funding for purposes including creating the ISAC, supporting operations, increasing membership, developing metrics, and providing for additional capabilities. According to ISAC officials, some have already received federal funding: the Public Transit ISAC initially received a $1.2 million grant from the Federal Transit Administration to begin operations, and the Water ISAC received a $2 million grant from EPA for fiscal year 2004 to cover annual operating costs and expand memberships to smaller utilities. In addition, the Financial Services ISAC received $2 million from the Department of the Treasury to help establish its next-generation ISAC and its new capabilities, including adding information about physical threats to the cyber threat information it disseminates.

Despite such instances, funding continues to be an issue, even for those that have already received government funds. For example, the Healthcare Sector Coordinating Council, which is the sector coordinator for the healthcare industry, is currently looking to the federal government to help fund the creation of a Healthcare ISAC. Also, officials at the Public Transit ISAC noted that funding is an ongoing issue that is being pursued with DHS. Officials at the Financial Services ISAC, who notes that the ISAC's goal is to become totally self-funded through membership fees by 2005, are also seeking additional government funding for other projects.

The ISAC Council has also suggested that baseline funding is needed to support core ISAC functionalities and analytical efforts within each sector. The Council's suggestions include that the government should procure a bulk license for the ISACs to receive data directly from some vulnerability and threat sources and access to analytical or modeling tools and that the funding for an ISAC analyst to work at DHS to support analysis of sector-specific information or intelligence requirements.

According to the Financial Services ISAC, DHS has agreed to fund tabletop exercises for some ISACs. For example, according to DHS officials, exercises are occurring this week involving the Banking and Finance sector and exercises for other sectors are currently being explored. In addition, energy sector-related exercises were held earlier in the year. DHS officials also stated that funding considerations for the critical infrastructure sectors and the ISACs would be based on their needs.

Utilizing Sector Expertise

In our discussions with ISAC officials, several, such as officials from the Surface Transportation and the Telecommunications ISACs, highlighted their analysis capabilities and, in particular, their analysts' sector-specific knowledge and expertise and ability to work with DHS and other federal agencies. The ISAC Council also emphasized that analysis by sector specific, subject matter experts is a critical capability for the ISACs, intended to help identify and categorize threats and vulnerabilities and then identify emerging trends before they can affect critical infrastructures. Sector-specific analysis can add critical value to the information being disseminated, with products such as 24/7 immediate, sector-specific, physical, cyber, all threat and incident report warning; sector-specific information and intelligence requirements; forecasts of and mitigation strategies for emerging threats; and cross-sector interdependencies, vulnerabilities, and threats.

The Council also emphasized that although government analytical efforts are critical, private-sector analytical efforts should not be overlooked and must be integrated into the federal processes for a more complete understanding. The private sector understands its processes, assets, and operations best and can be relied upon to provide the required private-sector subject matter expertise.

In a few cases, the integration of private-sector analytical capabilities with DHS does occur. For example, the Telecommunications ISAC, as part of Participation in National Homeland Security DHS's National Communication System, has watch standers that are part of the DHS operations center and share information, when the information owner allows it and when it is appropriate and relevant, with the other analysts. In addition, a Surface Transportation ISAC analyst also participates in the DHS operations center on a part-time basis to offer expertise and connection to experts in the field in order to clarify the impact of possible threats.

Participation in National Homeland Security Exercises

The ISAC Council highlighted the need for ISAC participation in the national-level homeland security exercises that are conducted by the federal government, such as DHS's May 2003 national terrorism exercise (TOPOFF 2), which was designed to identify vulnerabilities in the nation's domestic incident management capability. However, according to the Council, there has been little or no integration of active private industry and infrastructure into such exercises. For example, private industry participation in TOPOFF 2 was simulated. The Council believes that with such participation, both national and private-sector goals could be established during the creation of the exercise and then addressed during the exercise.

The Council did identify examples where the private sector is being included in exercises, such as efforts by the Electronics Crime Unit of the U.S. Secret Service to reach out to the private sector and support tabletop exercises to address the security of private infrastructures. Further, according to a DHS official, the department has agreed to fund tabletop exercises for members of several ISACs, including Financial Services, Chemical, and Electricity, as well as a cross-sector tabletop exercise.

Additional Challenges

Additional challenges identified by our work and/or emphasized by the ISAC Council included the following.

- **Obtaining Security Clearances to Share Classified Information.** As we reported last year, several ISACs identified obtaining security clearances as a challenge to government information sharing with the ISACs. Seven of the 15 ISACs with which we discussed this issue indicated either that some of their security clearances were pending or that additional clearances would be needed.
- **Identifying Sector Interdependencies.** Federal CIP policy has emphasized the need to identify and understand interdependencies between infrastructure sectors. The ISAC Council also highlighted the importance of identifying interdependencies and emphasized that they require partnerships between the sectors and the government and could only be modeled, simulated, or "practiced" once the individual sectors' dynamics are understood sufficiently. The current short-term focus for the ISACs is to review the work done by the government and the sectors regarding interdependencies. Similarly, a DHS official acknowledged the importance of identifying interdependencies, but that it is a longer-term issue.
- **Establishing Communications Networks.** Another issue raised through the ISAC Council's white papers was the need for a government-provided communications network for secure information sharing and analysis. Specifically,

the Council suggested that although functionality would be needed to satisfy the ISACs' requirements, DHS's Critical Infrastructure Warning Information Network (CWIN) could be used as an interim, first-phase communications capability. According to the Council, some of the ISACs are conducting routine communications checks at the analytical level in anticipation of expanded use of CWIN. In discussing this issue with a DHS official, he said that ISAC access to a secure communications network would be provided as part of the planned Homeland Security Data Network (HSDN). DHS recently announced a contract to initiate the implementation of HSDN, which is be a private, certified, and accredited network that provides DHS officials with a modern IT infrastructure for securely communicating classified information. According to DHS, this network will be designed to be scalable in order to respond to increasing demands for the secure transmission of classified information among government, industry, and academia to help defend against terrorist attacks.

DHS Information-Sharing Plan

At the time of our study, the relationship and interaction among DHS, the ISACs, sector coordinators, and other sector-specific agencies was still evolving, and DHS had not yet developed any documented policies or procedures. As we discussed earlier, HSPD–7 requires the Secretary of Homeland Security to establish uniform policies for integrating federal infrastructure protection and risk management activities within and across sectors. According to a DHS official, the department is developing a plan (referred to as a "roadmap") that documents the current information-sharing relationships among DHS, the ISACs, and other agencies; goals for improving that information-sharing relationship; and methods for measuring the progress in the improvement. According to this official, the plan is to define the roles and responsibilities of DHS, the ISACs, and other entities, including a potential overlap of ISAC-related responsibilities between IAIP and the Transportation Security Administration. Further, the official indicated that, in developing the plan, DHS would consider issues raised by the ISAC Council.

In summary, since first encouraged by federal CIP policy almost 6 years ago, private-sector ISACs have developed and evolved into an important facet of our nation's efforts to protect its critical infrastructures. They face challenges in increasing their sector representation and, for some, ensuring their long-term viability. But they have developed important trust relationships with and between their sectors—trust relationships that the federal government could take advantage of to help establish a strong public/private partnership. Federal agencies have provided assistance to help establish the ISACs, and more may be needed. However, at this time, the ISACs and other stakeholders, including sector-specific agencies and sector coordinators, would benefit from an overall strategy, as well as specific guidance, that clearly described their roles, responsibilities, relationships, and expectations. DHS is beginning to develop a strategy, and in doing so, it will be important to consider input from all stakeholders to help ensure that a comprehensive and trusted information-sharing process is established.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions that you or members of the subcommittee may have at this time.

If you should have any questions about this testimony, please contact me at (202) 512–3317 or Ben Ritt, Assistant Director, at (202) 512–6443. We can also be reached by e-mail at daceyr@gao.gov and rittw@gao.gov, respectively.

Other individuals making key contributions to this testimony included William Cook, Joanne Fiorino, Michael Gilmore, Barbarol James, Lori Martinez, and Kevin Secrest.

Mr. THORNBERRY. Thank you, sir. I appreciate your much more detailed written statement which I read last night, that goes into considerably more detail.

Mr. McCurdy, if you can do 5 minutes, we will go ahead and have you at it.

STATEMENT OF THE HONORABLE DAVE MCCURDY, EXECUTIVE DIRECTOR, INTERNET SECURITY ALLIANCE

Mr. MCCURDY. Mr. Chairman, I am used to a 2-minute rule, actually.

[Laughter.]

I will submit even the summary of my statement for the record as well. Let me just briefly, as I understand what the subcommittee is interested in. The Internet Security Alliance was actually formed in April 2001, 5 months before 9–11. I was actually in Tokyo at an OECD meeting on 9–11 defining cyber security best practices. So we have been at this for quite some time.

We formed a novel model. We had looked at the ISAC models and we in industry, in representing the Electronic Industries Alliance of over 2,500 member companies, found that those models were not sufficient for the needs of industry in improving cyber security. We created a cross-sectoral international organization that integrates many of the security services into one coherent model. The Internet Security Alliance is structured in a fundamentally different way than the traditional ISACs.

Let me just briefly say what they are. Cross-sectoral, we have members from the financial industry, from insurance, telecommunications, defense and security industries, consumer electronics, food products, and even the National Association of Manufacturers that represents over 12,000 companies. We designed the organization this way because quite frankly the Internet is structured this way, cross-sectoral. It knows no borders. It knows no boundaries, whether it is national or international. A cyber-attack on the Internet affects a lot of these companies the same way. I do not care if you are AIG, Coca–Cola, Sony, Verizon or Visa, all of whom are members of the Internet Security Alliance.

I said it is international. We have members on four continents. These are trusted partners, but they are dealing with similar concerns, and that is consistent with the national plan to secure cyber space. We are also developing security anchor programs in Latin America and other countries such as India.

Finally, our model attempts to provide, when I say a comprehensive, coherent and integrated approach to cyber security, we go beyond just information sharing. We had a partnership with the CERT/CC. I serve on the board of advisers for the Carnegie Mellon Software Engineering Institute and developed this relationship over quite some time on how they could improve their dissemination of information and get the feedback from industry.

We developed best practices. We are in our third practice book that just came out for small businesses. We had one for corporate leadership, the CEO-level leadership in major companies, and we had one for individual users. We have teamed with groups in order to make that work. We get that information from industry, working to build on the research also at Carnegie Mellon. These practice editions have been endorsed by TechNet and Partnership for Critical Security, NAM, the U.S. Chamber, and others.

In addition to that, we believe that wide distribution is critical, but currently it is not being done sufficiently. So we have developed some market-based incentives and some programs to try to get higher buy-in from the industry leadership. We have developed a program with AIG insurance where you have discounts if you follow best practices. There are tools being developed by a consortium on security trying to have metrics by which they can even determine whether or not there is a qualified member in order to participate.

Finally, a lot of this I think when people think of cyber, they think it is only an IT issue. It is both a physical and an IT issue.

They are interlinked. We have been doing this for some time. TIA, Telecommunications Industry Association, is our sector association in that space, and they have been a sector leader on critical infrastructure long before 9–11 or the recent concerns.

We are also working on risk management relationships and initiatives with industry. Lastly, I think the headline from this hearing and the question you really have is, how are we working with DHS? I commend DHS for their efforts. They finally have staff on the ground in place, and I think they are looking at developing plans. They appear to have decided on the ISAC Council as their prime link to the private sector, but the ISACs, while critical elements in this struggle, quite frankly do not represent everyone.

My concern from my experience, having sat where you do in this very room for many, many hours, I can assure you that government's approach is often silo-based and that is part of the problem that we have seen in dealing with government institutions and sharing. We decided we had to reach beyond that. That is why we created the Internet Security Alliance. We want to work with DHS. We want to be fully integrated into their discussions and we want to be full members of the partnership, whether that means that we are a cross-sector ISAC at some point of a tier-one partner. We do not know what the classification should be, but we do reach out. We have a great deal of experience.

We also have a great deal of experience with the CERT/CC on how we can help them improve the type of information which is relevant to industry. We were talking about information overload. I get emails every single day with another alert. There were four this morning, as a matter of fact. I think there is a way to narrow those. Mr. Dacey mentioned conference calls. We want to analyze the information and we pull groups together that actually take these alerts and translate them to meaningful, actionable items that the corporate sector or industry can actually work to improve their security.

Again, I appreciate the opportunity. I look forward to working with you all. I commend you for your efforts. I know how serious you take this and how important it is for the nation. Again, this is just not a national issue. This is cross-border. It is international. We think we have opened the way to help address the bigger plan, the bigger strategy of reaching other countries as well.

Thank you.

[The statement of Mr. McCurdy follows:]

PREPARED STATEMENT OF THE HONORABLE DAVE MCCURDY

Thank You Mr. Chairman.

My name is Dave McCurdy. I am President of the Electronic Industries Alliance and Executive Director of the Internet Security Alliance (ISAlliance).

I am delighted to be here today to discuss how the federal government can improve its coordination with the private sector and thus, improve worldwide information security.

As a cross-sector, international organization, which integrates many different security services into one coherent model, the Internet Security Alliance, is structured in a fundamentally different way than traditional Information Sharing and Analysis Centers (ISACs). We believe this model has much to recommend, not as a substitute for the ISACs, but as a complement to them. I am concerned, however, that we are not yet seeing this potential realized. Greater involvement and coordination with the ISACs and the Department of Homeland Security (DHS) would be extremely helpful to organizations like the ISAlliance, and the companies they represent and I believe would be in the best interests of our own national security.

Today I would l like to cover three main points.

1. I would like to outline the model the Internet Security Alliance operates under and suggest some fundamental differences from the traditional ISAC model.
2. I want to discuss how this model facilitates the development of an integrated, comprehensive, and coherent approach to cyber security, and I want to offer a couple of examples of how this approach can enhance our efforts to promote cyber security.
3. I want to raise some organizational issues regarding DHS coordination with models such as ours. I believe that organizations such as our need to be fully integrated into the public private partnership between DHS and the private sector either as an inter-sectoral ISAC or with equivalent status within the tier one partnership with the ISACs.

Before I begin I want to make our posture with respect to the ISACs very clear. About a quarter of our membership also participates in ISACs. Some of our Board members also serve on the Boards of various ISACs. We regard the ISACs as "comrades in arms."

It is surely true that there are some issues unique to industry sectors that are most effectively dealt with by a sector specific domestic entity. However, the ISAlliance also concurs with the National Strategy to Secure Cyber Space that found that "some cyber security problems have national implications and cannot be solved by individual enterprises and sectors alone."

We do not seek to displace the ISACs; we seek to work more closely with them, and DHS.

THE INTERNET SECURITY ALLIANCE MODEL

CROSS-SECTOR INFORMATION SHARING & ANALYSIS AVAILABLE TO ALL

The ISAlliance was created in April of 2001, five months before the attacks on the Pentagon and the World Trade Center. We created it because, even then, we saw the need for a new approach to the growing cyber threat.

In contrast to the ISACs, which are generally structured along traditional industry specific silos, the ISAlliance has members from many different sectors. We designed the organization this way because the Internet is organized this way. Essentially, we are all using the same Internet. So, from the cyber security perspective the threats and attacks may be very similar regardless if you are Coca-Cola, Sony, Visa or VeriSign (all members of ours). As a result, there is much to learn from, and help can be offered to, your brother companies regardless of industry sector.

As a member of the Board of Advisors of the Software Engineering Institute at Carnegie Mellon University, I have had substantial contact with the experts at the CERT/cc at Carnegie Mellon who educated me on this growing problem in 2000. We decided then that the private sector needed to not only contribute to, but to demonstrate leadership in making this critical infrastructure more secure. We devised a creative public private partnership, which integrated and maximized the complementary assets of CERT, the federal government and private industry.

CERT/cc, which was funded primarily by the U.S. federal government, had long been recognized as the premier center for Internet threat and vulnerability information. But it lacked a practical channel to get this information to the private sector, or stimulate interest in the necessary education, training, policy development and incentive programs that would be required to fully achieve the goal of information security.

EIA has been involved in physical security through the Telecommunications Industry Association (TIA) which is both a sector of EIA and an ISAC sector coordinator. Since we understood that physical and cyber security are most effectively dealt with in an integrated fashion, we sought a mechanism to bring these entities together.

We decided on collaboration between CERT/cc and EIA called the ISAlliance. Using the EIA member companies as a marketing base we recruited corporations to join the ISAlliance. They paid dues, and in return, operating under strict non-disclosure agreements would receive access to prime CERT/cc information. They would share this information with each other and the CERT/cc to identify and analyze looming threats and collectively work on solutions.

Since the ISAlliance members were receiving more from CERT/cc than the general public they agreed to pay a fee for this benefit. It was seen as a user fee similar to that paid by patrons at National Parks. While some companies using other, non-CERT, the ISAlliance services paid substantial dues, we never wanted money to be a barrier to entry into the ISAlliance. Dues entitling companies to the same CERT/

cc information (albeit fewer copies) were set as low as $3,000 a year—affordable for virtually any private firm. And, though we don't like to publicize it for obvious reasons, we have made financial adjustments for companies who had difficulty making the specified dues payment.

INTERNATIONAL

The ISAlliance is also focused internationally, where ISACs tend to be U.S.—centric. The ISAlliance has members on four continents. Our current Chairman of the Board. Dr. Bill Hancock, is from a British company and we have four other non-U.S. based companies on our Board along with eleven U.S. based companies. The international aspect of our efforts is important because cyber security is inherently an international issue. Many attacks originate offshore and implementing a truly effective means of securing cyber space must include finding and working with trusted offshore partners.

As the U.S. National Strategy to Secure Cyber Space states, in part; "America's cyberspace is linked to the rest of the world". . . . Securing global cyber space will require international cooperation to raise awareness, increase information sharing, promote security standards. . .The United States will seek the participation of U.S. industry to engage foreign counterparts in peer-to-peer dialogue with the twin objectives of making an effective business case for cyber security and explaining successful means for partnering with government on cyber security."

I'd like to offer a quick example of our efforts. After making a presentation to the Organization of American States (OAS) first broad conference on cyber security last August, OAS staff requested that the ISAlliance construct a specific program to integrate the private sector in the OAS region into the state-to-state programs for cyber security that were being developed. We came up with what we call our "Security Anchor" program.

This program is built on the "Transition Partner" program developed at Carnegie Mellon University. Under the Security Anchor Program private sector entities would obtain a special membership with the ISAlliance, which will allow them to essentially become "branch offices" within their regions. The Security Anchor for the region would distribute appropriate information about threats and vulnerabilities and hold meetings and conferences, but on local time providing translation as necessary for materials. The Anchor "tenant" would also be required to send personnel to Carnegie Mellon where they would be trained as trainers. The Anchor would then provide this training in their region, for which they could receive payment. We believe providing a market incentive to our Anchor partner is the most efficient and effective way to accomplish the goals set forth in our National Strategy.

In this way we hope to make international cyber security "home grown." We believe this is the only way that we can hope to succeed in reaching the international goals as set forth in the National Strategy. The U.S. can't expect to "export" security.

AN INTERGRATED COMPREHENSIVE AND COHERENT APPROACH TO CYBER SECURITY USING MARKET FORCES AS INCENTIVES

The ISAlliance attempts to provide its members with a comprehensive, coherent and integrated approach to cyber security that uses market forces to drive on-going improvements in cyber hygiene.

INFORMATION DISSEMINATION AND ANALYSIS

Like many ISACs, we begin with information dissemination and sharing about emerging threats, vulnerabilities and attacks on the Internet. We have historically done this though a contractual relationship with the CERT/cc as a founding partner in the ISAlliance.

In our three years of operations we have sent out literally thousands of these notices. We just released our first quarter technical report to the membership, which showed that in 2004 alone we have already sent out through our e-mail channel hundreds of reports, which have been followed by scores of analytical conferences between the members and CERT/cc.

When we, started several years ago, our prime activity was information sharing, mostly through e-mail notices. However, experience has taught us that simply disseminating information is by no means enough. In fact, our members have told us that at times there is too much information being circulated and the real need is to be able to separate out what is important and what is simply noise.

Information analysis is critical if threat and vulnerability data is to be used effectively. We facilitate the analytical process with regularly scheduled, as well as specially scheduled, meetings where in our members discuss the state of the network with the CERT/cc professionals. We have found the regularity of this process creates, over time, a sense of trust and confidence that we think is vital for effective information sharing.

DEVELOPING BROADLY ENDORSED BEST PRACTICES

While information sharing and analysis is a critical first step on the road to cyber security, is not sufficient to secure cyber space. Virtually every recent major attack we have experienced such as Blaster, Slammer, or MyDoom, resulted from a vulnerability, which was already well known, in the community.

At the ISAlliance we took the collaborative process of sharing information and built from it a systematic program of best practices. The process of developing the best practices is lead by the experts at Carnegie Mellon and CERT/cc and is consistent with the years of grounded research they have done and the theory of security that has evolved from their experience and analysis.

However, we also involve the full membership in our processes, so that the perspectives of actual businesses from multiple sectors and counties are folded into the final product. One advantage of this inclusive process has been that our practices have received an impressive level of support and endorsement from a wide breadth of the user community.

For example, our first publication, “The Common Sense Guide for Senior Managers” was endorsed by the National Association of Manufacturers (NAM) which represents 12,000 of the most traditional of industries, as well TechNet which primarily represents the high-tech companies in Silicon Valley. Internationally it has been translated into Spanish and Japanese and was endorsed by the U.S. India Business Council and distributed by the Organization of American States.

CREATING MARKET INCENTIVES TO ENCOURAGE ADOPTION OF BEST PRACTICES—THE QUALIFIED MEMBER PROGRAM

However, developing best practices is also not enough. CEOs are overwhelmed with information. To succeed with them on this subject, which has traditionally been viewed as a “cost center,” you have to do more than just tell them it’s the right thing to do. We have to talk about issues they care about, like profitability, liability protection and marketing. We need to develop market incentives to increase the Return on Investment (ROI) for cyber security.

The ISAlliance has taken the lead on this issue. In the final quarter of 2003 we signed an agreement with AIG, which is the world’s market leader in cyber insurance. Under this new agreement AIG will provide insurance premium credits of up to 15% for companies that will join the ISAlliance and subscribe to our best practices. We believe this is the first operating program which specifically ties a widely, and independently endorsed set of cyber security best practices directly to lower business costs.

We are working through AIG and the Global Security Consortium (GSC), comprised of the big auditing and accounting firms, on empirical standards with which we will be able to use to measure compliance with these practices. Not only will this tool enable us to more reliably determine who qualifies for the credits, but also it opens up another potential market incentive for improved security. We want to interest firms in marketing cyber security.

Firms that achieve a specified score will be deemed a “Qualified Member” allowing them to use that designation as a market differentiator. Through this mechanism we hope to make cyber security a useful marketing tool for good actor companies, much like the Baldrige Award has been used for high quality companies. GSC hopes to have their tool completed shortly and then this phase of the program can begin.

DISCOUNTED EDUCATION AND TRAINING COMPLETE THE LOOP

Finally, for firms who don’t yet score at an appropriate level to qualify for our discounts, we offer access to a wide range of training programs through Carnegie Mellon University. In keeping with the market orientation of our program, the more active a company is in the ISAlliance, the greater the discount they can receive on their training. Our interest is to accurately inform organizations where they stand in relation to the widely endorsed best practices, and help them reach an appropriate level if they are not already there. Most importantly, the people doing the training are operating on the same assumptions and best practices that we started with in the first place thus creating a truly coherent program.

BEST PRACTICES FOR SMALLER BUSINESSES

This program is just one example of our activities. In fact, this afternoon we will be testifying before another Committee on a similar program, this time specifically targeted to the unique needs of smaller businesses. The National Cyber Summit, recognizing the value of programs such as I have just described, and realizing that there was not nearly enough being done to reach out to smaller businesses, asked us to undertake this new effort this past December.

Although smaller businesses have not until now been our prime market interest we agreed to take up the challenge. Working with the U.S. Chamber of Commerce, the National Federation of Independent Business (NFIB) and NAM we followed the same integrated, market centered model we described above. We held ten focus groups involving nearly 100 small businesses to find out what needed to be done to improve their cyber security.

What we learned was that smaller institutions are indeed different from larger ones. In fact, we found that organizations across a wide spectrum of business types had remarkably similar problems from a cyber perspective. The similarities for these businesses were not the type of business they were in, but the size of their business and the extent of the technology available to them. As a result, the "Common Sense Guide to Cyber security for Small and Medium Sized Businesses" looks quite different from the Guide for Senior Corporate Managers.

We are happy to report that what was not very different is the response, which has been extremely positive. Already the Cyber Security Partnership that grew out of the National Cyber Summit as well as on the web sites for the ISAlliance, the Electronic Industries Alliance and the National Association of Manufacturers is distributing the Small Business Guide. The U.S. Chamber of Commerce has informed us they expect to endorse the document at their next Board of Directors meeting and the Financial Services Sector Coordinating Council, an alliance of 28 financial services trade associations will be making it available to their members and holding a series of meetings with thousands of its members where the Guide will be highlighted.

Given the fact that this project is only a couple of months old we are naturally very encouraged. When mature, we fully expect this program will be coherent, measurable and market driven just as was the case with the Senior Managers program.

CYBER AND PHYSICAL SECURITY—REACHING OUT TO RISK MANAGERS

Another area we are working on is the integration of cyber and physical security. We believe, as Secretary Ridge has said, that you can't have cyber security without physical security and you can't have physical security without cyber security. However, in corporate America there remains a misconception that cyber security is an "IT problem." While obviously there are many IT aspects to cyber security it is not properly classified only as an "IT problem."

Cyber security is a management problem. It is an economic problem. It is an employee training, compliance and retention problem. Most of all, cyber security is a risk management problem. However, most corporate structures still relegate the discussion of cyber security to the IT department rather than fully integrating it into the discussions with physical security and risk management. We have heard a good deal of talk recently about structures within the federal security bureaucracy which may have limited information sharing and proper threat management. Private industry is not immune to these same types of organizational problems.

Therefore, we have recently undertaken a pilot study reaching out to the risk managers in industry in an attempt to find out how we can better involve them in the cyber security discussion. We believe that it's critical to better integrate physical and cyber security issues within the overall corporate risk management structure. We are trying to find out how we can do that, from the people who are actually making the organizational, budgeting, and resource allocation decisions.

Although we have initiated this study, it is too early to report results. We do expect however, that, as was the case with our other projects, we will learn from this effort and we can make further impact in securing cyber space. We look forward to sharing these approaches both with industry, and to the federal government.

NOT JUST SERVICES; A COHERENT INTEGRATED PROGRAM

We believe the comprehensiveness of the ISAlliance program is making a positive contribution to the cause of information security.

- Hundreds of technical notices about Internet threats and vulnerabilities each year to our members from the best source available to private industry.
- Scores of analytical conferences to discuss the data and what to do about it
- Development of best practices that are widely endorsed and disseminated both domestically and abroad.
- Development of independent, auditable third-party evaluation tools and methods
- A program of market-based incentives to improve the ROI for cyber security
- Education, training and public policy programs.
- Initiating new programs to push the envelope into heretofore underserved populations

But the key aspect is that it is a coherent program. We start with the hard data we get from CERT and we blend into that the real world needs and experiences of industry and develop programs, practices and policies which can drive pragmatic improvements. And then, if individual entities can't make the grade they are offered training based on the same theories and practices that were used to develop the best practices.

COORDINATING WITH THE ISACS AND DHS

As proud of these accomplishments as we are, we have some concerns for the future.

We supported, and continue to support, the creation of the Department of Homeland Security. We in no way wish to be critical of the effort and sincerity of the people who are working at DHS. They are working very hard to accomplish an enormous task virtually immediately. We sincerely hope that our testimony at this point will be taken in the spirit it is given, constructive suggestions that we believe will assist all of us who are working in this space to be more effective.

In fact the ideas we offer the Committee today have been previously raised with staff and principals and we are continuing to work on them. We anticipate that in the due course of time they will be satisfactorily resolved. We believe, however, that there are very important issues, which must be appropriately addressed.

DHS SHOULD COORDINATE WITH ALL INFORMATION SHARING ORGANIZATIONS—NOT JUST ISACS

We suggest DHS broaden its systematic communication to include organizations, such as the ISAlliance, who are providing important services, although they are not ISACs.

In the interdependent cyber world the "critical infrastructures" may be dependent on the "non-critical" organizations that service them. In addition to the IT, telecom and financial institutions we represent we count the National Association of Manufacturers among our sponsors. These are the people who manufacture the parts used to construct our defense products and operate the supply chains upon which many "critical" businesses rely. These organizations also need to be systematically included in the on-going public private partnership with DHS.

Moreover, while we are focused on cyber security today from a national security perspective, most Internet attacks have nothing to do with international terrorism. Cyber security is also a critical business issue and from a business perspective the "non-critical" portions of the economy deserve as much protection as the rest of the economy.

The Department of Homeland Security seems to have decided upon the ISACs and the ISAC Council as the primary linkage to the private sector. Since we are not formally an ISAC, we are not part of the ISAC Council and hence we are not in many of the meetings and discussions from which DHS appears to be receiving their primary input. We would like to work with DHS and the ISAC Council to integrate our broad membership into this forum.

Two years ago Congress passed legislation, which attempted to facilitate the sharing of information between private industry and the government. In the initial drafts of that bill the adjustments to FOIA, etc. were confined to ISACs. It was correctly pointed out to the drafters that there is in fact information sharing outside of the formal ISAC structure and the legislation was redrafted to read "information sharing organizations." We believe DHS should follow this precedent in developing their public private partnership.

COMPANIES NEED THE CERT/CC DATA THEY HAVE COME TO RELY ON

Over the past several years the nearly 60 companies who are members of the ISAlliance have come to rely on our working relationship with CERT/cc. Last year, DHS announced that they would be launching USCERT utilizing in main the facilities formerly known as CERT/cc at Carnegie Mellon.

We have no objection to DHS creating USCERT. Indeed, we see it as following and extending the model we created over three years ago for how to disseminate CERT/cc data to the private sector.

However, it would be problematic if suddenly the ISAlliance members who have relied on this information to build their corporate security plans and policies, are now denied access to that data.

Indeed, such an outcome could result in a substantial reduction in corporate cyber security as companies scramble to find alternative ways to receive this information. Moreover, the fact that this data might now be available though an ISAC is not an answer since the majority of the ISAlliance members, do not participate in ISACs

We would like to work with DHS to assure that the transfer from CERT/cc to USCERT and their new partners does not ironically result in less information being available to some worthy companies.

I want to conclude by noting that DHS has been open to meeting with and discussing ways to coordination with us. Just a few weeks ago I met privately with Assistant Secretary Liscouski who was most gracious and cooperative. I also want to single out Director Yoran, who has been especially helpful and has directed that at least for the short term the ISAlliance not be denied access to the data its membership has come to rely on. We are now hoping to finalize an appropriate long-term solution. Moreover, DHS staff have attended meetings with our membership and been very supportive. We want to thank and congratulate the whole team at DHS for their commitment and efforts.

And finally I want to thank you, Mr. Chairman and the joint Committee for all your work and for holding this hearing this morning.

Mr. THORNBERRY. Thank you. A lot of issues to pursue. This hearing will stand in recess until five minutes after the conclusion of these votes. It will be more than 30 minutes, so if you all have a chance to go get something to eat or whatever, please do.

We stand in recess.

[RECESS]

Mr. THORNBERRY. We are going to go ahead and get started. I think Mr. McCurdy will be back shortly. Apparently, he went down to have a sandwich and probably had long lines.

Thank you all again for your patience. Ms. VanDe Hei thank you particularly for yours. Now, we will turn to you and give you an opportunity to summarize your statement and then we will turn to questions.

STATEMENT OF DIANE VANDE HEI, VICE CHAIR, INFORMATION SHARING AND ANALYSIS CENTER COUNCIL

Ms. VANDE HEI. Thank you, Mr. Chairman. I assume that my written testimony will be part of the record. The summary can be as well.

Mr. THORNBERRY. Previously, we had unanimous consent for all full written statements to be made part of the record.

Ms. VANDE HEI. I am also assuming you have saved the best for last, so I thank you, Mr. Chairman.

Mr. THORNBERRY. Absolutely. Let me just say this, we are much more relaxed on time now. We have no more votes today, so that may work to your benefit or your detriment, depending on how you look at it.

Ms. VANDE HEI. Thank you, Mr. Chairman and distinguished members of the subcommittees. It is an honor for me to be here today to talk with you about the private sector's relationship with the Department of Homeland Security. My name is Diane VanDe Hei. I serve as the vice chair of the ISAC Council. I also serve as the executive director of the Association of Metropolitan Water Agencies and the WaterISAC, Water Information Sharing and Analysis Center.

In the way of background, the ISACs originated when the Federal Government issued its policy on critical infrastructure protection, otherwise known as Presidential Decision Directive 63. That directive carried through to the new Administration but it is now embodied in a new directive called HSPD–7. I cannot tell you what it stands for, but we do pay attention to what it says. It continues the emphasis on ISACs and the need to share information.

The ISAC Council brings together 14 sectors at this point, including the eight originally designated critical infrastructures. We have tried to be inclusive, rather than exclusive, wanting to learn from each other. The goal of the ISAC Council is to look at not only how we can learn from each other in terms of the models we use, but also to look at interdependencies. We have formed trusted relationships with the other sectors including electric, rail sector, and others so that if something happens to them, they can work with us. One of the primary goals of the ISAC Council was to build that kind of trusted relationship among sectors, but also to begin to look at how we could better share information with the government and the government could share it with us.

To improve the ISACs and to help communicate with government, the ISAC Council has developed eight white papers that reflect the collective analysis of the members of the ISACs and cover a broad set of issues and challenges. These papers recognize the critical leadership role played by the private sector with respect both to the organizational structure established in the ISAC, for analysis and information sharing, and in the interaction of the ISACs with the Department of Homeland Security and other government agencies addressing the challenges of infrastructure protection. We have shared these papers with Hill staff, DHS and GSA.

One of the primary challenges to government and the private sector is the establishment of a trusted partnership. You have undoubtedly heard that a number of times. As I think you all know, trusted partnerships cannot be legislated, regulated or even stipulated, nor can partnerships be purchased, traded or incorporated. We have learned that our ISACs need the full support and confidence of certain key elements of government to create and maintain a successful comprehensive security strategy.

Furthermore, we are also keenly aware that we, the critical infrastructures, need to maintain a trusted relationship with our government partners so that we can work with them and their staffs to maintain the delicate balance between security and privacy. Our relationship with DHS has had a few bumps in the road, but overall we have progressed, and I believe have common goals and agree on the strong need to partner in information-sharing and analysis.

As with the maturation of DHS, so has each of our collective ISACs. I do believe that the government assisting the private sector with baseline funding for certain sectors is ideal. The WaterISAC, the one I am most familiar with, for example has received funding from Congress and the U.S. Environmental Protection Agency, while we as a sector continue to build the private sector contribution to the ISAC. Although the information on the WaterISAC is available to 54,000 community water systems and over 15,000 publicly owned waste water treatment facilities, our fee for service is based on populations served. We do not differentiate between the kind of information utilities receive, but we differentiate based on the size of the system. The range in price is from $500 a year to $7,500 a year.

By doing this, we hope to get all of the utilities subscribing to the ISAC. Having said that, that has not happened. So our next enhanced phase of the WaterISAC is going to be development of a push email service that will go to thousands of drinking water and waste water, utilities, a service that will send DHS and EPA notices and advisories that need to be sent out simply because that is the ethical thing to do. So we are working on that this year and hope to have the new system in place before the end of the year.

Other ISACs, as you might expect, are structured differently depending on the composition of the sector and the breadth and scope of the services that sector has decided is needed. Banking and finance is different from water is different from electric is different from telecom.

In addition, the DHS IAIP regularly meets with the ISAC Council and listens to many of our concerns regarding the need for their strong support of the ISACs and the improvement of our information-sharing capabilities.

If I could leave you with two recommendations, it would be these. We need your help to ensure that the private sector's investment in their ISACs is built upon and strengthened. I believe that once you lose this voluntary work, research that people have been doing, that it will be lost for good. So we need your help to ensure that the investments that have been made in building these things is built upon, used and enhanced.

Second, we need your help to insist that the private sector be included up front in the analysis of intelligence. Government must learn to trust infrastructure owners and operators with real information that allows us to apply our resources in a smart way to protect the infrastructures. Again, I will just give you a quick example. The WaterISAC employs analysts that have top security-plus clearances so that they can communicate with intelligence officials in order to provide insights into what its impact on water might be. Even with that capability, we find that it is after the fact that we are often involved, or allowed to participate in any sort of review into what a threat to our water system might be. So we could use your help in that manner as well.

That concludes my remarks. I would be glad to answer any questions you might have.

[The statement of Ms. VanDe Hei follows:]

PREPARED STATEMENT OF DIANE VANDE HEI

Introduction

Good afternoon, Chairman Thornberry, Chairman Camp, and distinguished members of the subcommittees. It is an honor and a privilege to meet with you today to discuss the private sector interaction with the Department of Homeland Security (DHS).

I would like to thank both the Cyber Security, Science, Research & Development Subcommittee and the Infrastructure and Border Security Subcommittee for creating this important opportunity and inviting the ISAC Council to be here today.

My name is Diane VanDe Hei. I serve as Vice Chair of the Information Sharing and Analysis Center (ISAC) Council. I am also Executive Director of the Association of Metropolitan Water Agencies as well as the Water Information Sharing and Analysis Center (WaterISAC).

Background

ISACs originated when the Federal Government issued its policy on Critical Infrastructure Protection, otherwise known as Presidential Decision Directive 63. PDD–63 has been replaced with HSPD–7, to authorize and encourage national critical infrastructures to develop and maintain ISACs between the private sector in cooperation with federal government as a means of strengthening security and protection against cyber and operations attacks.

The ISAC Council

Homeland security presents significant challenges for the ISAC community and we look forward to working directly with you in the coming months. The work you are doing is extremely important and you have the commitment of the ISAC Council to do everything we can to assist in protecting the critical infrastructures of the United States.

I am here today to briefly discuss the ISAC Council and its role in protecting critical infrastructures. Members of the subcommittees, the ISAC Council voluntarily formed almost two years ago. Our goals are to discuss interdependencies and how we can develop better communications—among the various sectors and across borders—as well as what information should be shared on both physical and cyber issues within the sectors and with the government.

The Council has grown from representing eight sectors to include 14 sectors. In addition to the private sector membership, the ISAC Council also includes government ISAC's such as Emergency Management and Response who report to DHS as well as the Multi-state ISAC.

Early on the ISAC Council saw the need to be a very inclusive group. Although each of our sectors is unique in composition they are also intimately intertwined with each other, and a catastrophe in one sector can impact many others. We have seen this on a number of occasions. Take 9/11 for example, we had a physical impact on the twin towers, which impacted telecommunications and electric services, as well as closing Wall Street for four business days. Additionally, the northeast power outage impacted several sectors including drinking water, wastewater, transportation and small businesses alike.

To improve the ISACs and to help communicate with government, the ISAC Council has developed eight white papers that reflect the collective analysis of members of the ISAC Council and cover a broad set of issues and challenges. The topics include:

- Government—Private Sector Relations
- HSPD–7 Issues and Metrics
- Information Sharing and Analysis
- Integration of ISACs into Exercises
- ISAC Analytical Efforts
- Policy Framework for the ISAC community
- Reach of the Major ISACs
- Vetting and Trust

These papers recognize the critical leadership role played by the private sector, with respect both to the operational infrastructures established in ISACs for analysis and information sharing and in the interaction of ISACs with the Department of Homeland Security and other government agencies addressing the challenges of critical infrastructure protection. We have shared these papers with Hill staff, DHS and GSA.

We believe that these papers are only the beginning steps in tackling the serious policy and process issues challenging the implementation of an effective private sector and government information sharing and analysis partnership. The ISAC Council is continuing to work on concrete actions to increase ISAC support to the nation. To facilitate this effort, the ISAC Council members communicate on a daily basis (conference calls or by email) on operations and on an as needed basis for large new vulnerability announcements and/or incidents.

Government—Private Sector Partnerships

One of the primary challenges to government and the private sector is the establishment of trusted partnerships. I believe we all agree that partnerships between government and the private sector are essential and since 9/11, it has become even more critical for these partnerships to mature in order to effectively address homeland security issues.

As you all know, trusting partnerships cannot be **legislated, regulated, or even stipulated.** Nor can partnerships be **purchased, traded or incorporated.**

Partnerships are built between people and organizations that recognize the value in joint collaboration toward a common end. They are **fragile entities** that need to be established and maintained by all participants and **built upon a foundation of trust.**

We have learned that our ISAC's need the full support and confidence of certain key elements of the government to create and maintain a successful and comprehensive security plan. Furthermore, we are also keenly aware that we, the critical infrastructures, need to maintain a trusted relationship with our government partners so that we can work with them and their staffs to maintain the delicate balance between security and privacy.

Our relationship with DHS has had a few bumps in the road, but overall we have progressed and, I believe, have a common goal and agree on the strong need to partner in information sharing and analysis.

As with the maturation of DHS, so have each of our collective ISAC's. I do believe that the government assisting the private sector with baseline funding for certain sectors is ideal. The WaterISAC, for example, has received funding from Congress and the U.S. Environmental Protection Agency (EPA) while we continue to build the private sector contribution to the ISAC. Although the information on the WaterISAC—available to 54,000 community water systems (90 percent publicly owned and 10 percent investor owned) and 15,000 publicly owned treatment works—is available to all subscribers, our fee for service to these utilities is tiered based on population served. By doing so, we hope to make the WaterISAC affordable to all drinking water and wastewater utilities. In addition with the help of congressional funding, this year we will broaden the reach of the WaterISAC by developing a push email system that will be capable of reaching thousands of drinking water and wastewater utilities with federal advisories and notices.

Other ISACs, as you might expect, are structured differently depending on the composition of the sector and the breadth and scope of the services the sector decides is needed. That being said, we must keep our ISAC models in tact, meaning that the government should not attempt to dictate how the individual ISACs are structured nor how information is provided analyzed and reported to government.

On a very positive note, DHS has agreed to pilot the HSIN network with the water and electric sectors and has also provided funding to do tabletop exercises with the Financial, Telecommunications, and Electric Sectors.

In addition, DHS IAIP regularly meets with the ISAC Council and listens to many of our concerns regarding the need for their strong support of the ISACs and the improvement of our information sharing capabilities.

Summary

The ISAC Council plays an important role in homeland security. It brings together diverse sectors, examines commonalties and most importantly cements trusting partnerships that allows us to share information, learn the best from each other and enhance communication among interdependent sectors.

If I could leave you with two recommendations it would be these: We need your help to ensure that the private sector's investment in their ISACs is built upon and strengthened. Once lost, this type of voluntary commitment will be very difficult if not impossible to rebuild. Secondly, we need your help to insist that the private sector be included "up front" in the analysis of intelligence. Government must learn to trust infrastructure owners/operators with real information that allows us to apply our resources in a smart way to protect the infrastructure.

Thank you for the opportunity to testify today. I would be happy to answer any questions.

Mr. THORNBERRY. Thank you.

Ms. Lofgren?

Ms. LOFGREN. I am interested, Ms. VanDe Hei, on how not every water entity belongs to the ISAC. Am I correct?

Ms. VANDE HEI. That is correct.

Ms. LOFGREN. So how do you disseminate and communicate with those entities that are part of the whole system, but not actually part of the ISAC?

Ms. VANDE HEI. From 9–13–2001, the first thing we did was to develop an email push system that could reach thousands of utilities. We maintain that today. So although the subscribers to the WaterISAC receive it, the WaterISAC is both the knowledge base that we house sensitive information on, and also a means of sending out encrypted email. At the same time, we have maintained the push email system that we had developed almost three years ago. So when need be, we just push it out.

This advanced system that I was talking about earlier where we were developing a new system where it would just be pushed out to thousands of utilities, we have the funds to do that today and we hope to have that by the end of the year. So we will be reaching both subscribers and those who do not join the WaterISAC.

Ms. LOFGREN. Looking at it from the other point of view, the information that DHS needs about threats, from what Mr. Liscouski said, they are dependent upon the entities involved. So you would have information about your part of the water world. How do you involve the rest of the water world that is not a part of the ISAC in that threat assessment activity? Are they asked to participate? How are they identified and included?

Ms. VANDE HEI. In the assessment of their individual utilities?

Ms. LOFGREN. We have yet to accomplish a comprehensive threat assessment.

Ms. VANDE HEI. Yes.

Ms. LOFGREN. What I think the testimony is that we are soliciting information from various entities in charge of aspects of American life about what the threat is. ISACs are part of that protocol, but not everybody who is a part of the world is a part of the ISAC. How do we include them? Do you play a role in that? Does the Department do it directly?

Ms. VANDE HEI. What we have done is we have included both on the secure site and on the public site an incident reporting form that anyone can fill out. It comes into the WaterISAC for the analysts to look at. That information is shared with the intelligence community, particularly if it looks like it is a pattern in a region. So we have it available both on the private site and the public site. So you could go to the public site and report an incident, and it would go to the analysts and be treated seriously.

Ms. LOFGREN. That may or may not be good news if it is a public site and the terrorists have access, too.

Ms. VANDE HEI. It will go into the system is what it will do.

Ms. LOFGREN. Have you, for example in your ISAC, been solicited for critical information, threat assessment information?

Ms. VANDE HEI. No. Drinking water systems are a little bit different in that they were required in 2002 to do vulnerability assessments and to provide them to EPA. So we know that the 500 largest systems serving over 100,000 people, those are done.

Ms. LOFGREN. Right, but we do not know whether DHS has actually availed themselves of that information.

Ms. VANDE HEI. We do not, but they are being treated as sensitive documents. I understand that they have requested the ability to view them. How often, how frequently, I am not privileged to that information.

Ms. LOFGREN. Just out of curiosity, thinking about this is structured, in California, if you know, who belongs to the ISAC in the water world? Who belongs and who does not belong in the WaterISAC?

Ms. VANDE HEI. I do not have that list with me today.

Ms. LOFGREN. Could you send it to me later?

Ms. VANDE HEI. Sure.

[No list provided to the Committee by the time of printing.]

Ms. LOFGREN. I appreciate that. Thank you very much.

I am interested, Mr. Dacey, on the ISACs, it is the same question. The Department of Homeland Security needs to reach out for this critical infrastructure assessment. Do you know what DHS is doing to reach out to non–ISAC entities for this information?

Mr. DACEY. I am not familiar with the exact actions they are taking, but I think that is certainly an area that has been identified by pretty much everyone as an area that needs to be addressed. If you look broadly across the ISACs when they were initially formed, although if you look at the numbers a large portion of the operations of the industry generally are represented, oftentimes that is concentrated in a relatively small number of entities that are the leaders in those industries. We have a large number, and we gave some examples in our testimony in financial services, a large number of entities that are not participants in the ISACs, but are members of the industry; that are important, but do not represent the same level of volume. So I think that has been a longstanding issue.

With respect to financial services, they actually worked with the folks at Treasury who is their sector-specific agency, and came up with what is called the next-generation ISAC, because their views were that this rebel population was not willing to pay a significant amount of money in order to participate in the ISAC. So they have developed a model where there is a certain basic level of services that are available free to all participants who want to join the ISAC and then have a tiered approach where you pay more at different levels to get a higher level of services. I think that is an issue that needs to be addressed. There are tiers in several of them, but not certainly across all of them. That is one of the areas that needs to be thought through as to how that will be accessed and how that information will be paid for, whether the Federal Government should continue to fund communications for this type of thing for that layer.

Additionally, there are some ISACs that have the funding actually to try to develop some of their operations, because again those were concerns about how they would fund their initial operations and set up, and then there was Federal funding to help that get started as well.

Ms. LOFGREN. I guess that raises a question of if the financial obligations are a barrier to participation and it is really in the interests of the Nation that people participate, whether we ought to put those, I mean, there is a dual purpose. The entity involved is going to benefit, but the reason why we were asking about these ISACs is to protect America against terrorist threats. If they are not participating because of the fee structure, perhaps we should not have that fee structure at all if we really want entities, both private and public, to participate.

Mr. DACEY. It gets back to the basic models. These were set up as voluntary organizations. To the extent that their respective memberships felt it was cost-effective, they funded those operations and provided the level of services that were appropriate for that particular sector.

Ms. LOFGREN. Right, but from their point of view.

Mr. DACEY. Exactly, from their point of view. That gets to the next question, well, if the Federal Government has expectations about the level of capabilities and services that are to be provided by these ISACs, that needs to be articulated and discussions entered into with industry as to how that would be paid for; whether incentives might be appropriate.

Ms. LOFGREN. Do you have a recommendation on how these might be changed? Would you think about whether you could give us a recommendation that would forward the government's interest in having sectors which are not currently participating participate?

Mr. DACEY. We certainly can look into that. We have a broad recommendation we have had out for a number of years, at least for a year, that the sectors needed to assess the need for additional public policy tools to provide the appropriate incentives for participation in ISAC and other CIP activities. So we have had that broad recommendation out starting basically in January and February of last year.

Ms. LOFGREN. And you think we could just adopt that and that would solve it?

Mr. DACEY. I think you need to think about this from a strategic level and think about how you want to do that, not that one size fits all. How do you want to apply those incentives to the sectors? I think you need some ground rules, some criteria, some structured process so that it is transparent as to how the government is going to go about doing that process.

Ms. LOFGREN. Right. OK, I want to think about that.

Finally, and I do not want to hog the time here, the Chairman is being indulgent and I am sorry I missed your testimony, Mr. McCurdy, and the two secretaries, but has the Department of Homeland Security met with the variety of industry partners that you represent to get their assessment of threat in this sort of quest for the holy grail of the threat assessment that we are waiting for?

Mr. MCCURDY. First of all, the Internet Security Alliance was formed, Ms. Lofgren, as a private, it was really the first public-private partnership, to be honest, because we teamed with Carnegie Mellon and Carnegie Mellon was running the CERT which was funded by the Department of Defense. Their incentive was to try to reach out to the private sector which had a lot of expertise, but it was not getting out to industries. Together, we came up with the new model of having the cross-sector relationship and international. There are 88 CERTs around the world, and yet there is not the kind of coordination that we felt was needed, nor was there the incentive in a lot of other countries to even involve the private industry, even though private industry owns about 85 percent of the infrastructure.

So DHS has gone through an evolution, as you know. As I stated in my earlier comments, we were officially launched 5 months before 9–11. We were formed prior to that. This was an effort from industry in trying to gain greater access to information that we felt was critical in this continuum of ensuring that the Internet itself, the best practices and the standards and the security, was increased.

DHS, I think now that they do have people in key positions, both Mr. Liscouski and Amit Yoran, have been more receptive to our involvement and to our comments. One of the critical points that needs to be raised, it is true, one size does not fit all. My concern, having spent as much time as I have in government, is back in the intelligence days and also in defense, there is a tendency to become stovepiped. We felt in this age that we had to cross-cut that.

The second thing is, somewhat to our chagrin, there has not been the level of concern by certain levels within industry, corporate leadership, to provide the funding or even the awareness that there was as much at risk. That is why we developed the best practices for the C-level entities and for the organizations, trying to raise this concern, and also have them ask themselves in their organizations and enterprises the questions that they should be asking to understand what their level of security is. The second point is, whether it is a push system or a pull system, I think there have to be incentives for industry to participate at certain levels. We have a fee structure. At one level, it is quite high, but we have more members than most of the ISACs. The reason they have joined, early on it was because they wanted access to the information, but we learned something in this multi-year process, now 3 years, and that was information alone is not enough. You need to be able to analyze it. You need to understand it. So we convened these working groups. If there is a call, they can quickly filter through and say, I do not have that particular information; SNMP is not my concern. OK? I will not participate in that call.

If I have a vendor or a system that relies on that, I can tell you that they will have active engagement in discussions, learning from the experts and from each other, and that information flows back towards government through the CERT. I think there have to be market-based incentives, and that is why we have started with the insurance program; that is why we are working with risk management; that is what we are trying to do with the anchor system, with trusted partners in other countries.

We actually when we began the Internet Security Alliance made a conscious decision really not to be involved with government. That was before 9–11. Post–9–11, it is obvious that industry, regardless of on which continent it resides, has to be engaged somewhat in this system. So I think there is not only increased awareness, but I think there is increased willingness to participate and not to be as concerned about the privacy of their data or what their receiving from government. It is not going to be quite as biased.

The last point I would make, if we could, it needs to be inclusive, not exclusive. There is a concern that a certain incumbency or PDD–63, whatever the foundation happened to be, that that is the model that is the model and will be the model. I think we need to explore a lot of different models. I think that is what Mr. Dacey and others have been saying. There are some that have worked quite well. We have gone beyond the basic information sharing to a whole new level. But if for some reason our members were cut off from that information flow, I think it would affect not only their business, but I think it would affect the security of the Internet.

Ms. LOFGREN. Is there legislation that we could adopt that would assist in providing incentives or disincentives to accomplish what you have outlined here?

Mr. MCCURDY. Government is usually quicker to have disincentives than they are incentives, especially in fiscally difficult times. I am sure there could be a combination. We would like to see it on the incentive side, because actually that is where our CEOs and others respond. There are research incentives. There could be incentives for implementing or employing certain technologies. There is the FOIA concern. There is liability, safe harbor kinds of issues that obviously provides some incentives.

Mr. Putnam had drafted legislation that he considered introducing. I think it was originally intended to be around the Y2K model, which worked. Unfortunately, it was starting to look more like Sarbanes–Oxley, which is a burden on industry, and actually you would get pushed back, and if anything you would actually deter people from being more open and responsive.

So we would like to find the right approach. Mr. Clinton, who is our chief operating officer, is going to testify later today before that committee, about some of the market-based incentive packages that we have developed. As far as I know, we are the only ISAC or information-sharing group or organization out there that has even gone that far. But we have gone beyond just best practices. We have published those and we are creating more.

Ms. LOFGREN. I have seen those.

Mr. MCCURDY. Yes. That is actually where government, if there was going to be funded and people talked about where this money is going to go, distribution actually costs money, in getting that out. We just produced one for small businesses. Who bears that cost? Those are our natural constituency, quite frankly, in my association, but we decided we had invested a great deal of money in the Internet Security Alliance to get it started and up and running. Ms. VanDe Hei mentioned the need to protect some of that private investment. Well, there has been a significant investment, and not always willingly, some of it because of my experience really pushing the industry to be on the cutting edge and up front before I think even some recognized that there was a threat. Now, they are starting to see it a little bit more.

Ms. LOFGREN. I will stop and let the Chairman ask his questions, but isn't it true that certainly there is a burden to participating in the ISACs on the part of any entity, private or public, just in terms of the personnel costs and the time taken from other tasks. That is a burden that may be easier to bear for a larger entity than a small entity. For a small business, that can become a daunting, in addition to the fees, just participating, and for a threat that is inchoate. There may not really be the business incentive. So it may not be occurring. So there is a cost to disseminating the information, but disseminating the information without incentives to actually implement is another issue, whether there would be insurance benefits, which has been discussed, or other benefits that would allow a small business person or persons or a small company to actually justify the expense and time away from other bottom-line activities.

Mr. MCCURDY. We learned a great deal in developing the best practices document for small businesses. On one level, they are similar vehicles. I mean, they are using the Internet, but their capability and their access to personnel, policies, technology is far different. You are right. It is a hurdle for many, not only in just cost, but also time. It is a real challenge to find the right incentive to get them involved.

We learned from some of our partners, our founding members, VISA for instance has what they call the digital dozen. They are in a different modality. They are able to require their merchants to meet certain practices. One of our other members, Nortel, has considered, I do not know if they have implemented, and I probably should not be speaking for them, but they want their supply chain, they want their suppliers to be at a certain level of security. So they are encouraging them not only to belong to Internet Security Alliance, but also to meet certain best practices.

So there are a lot of companies and a lot of entities are doing it differently, but that does not mean it is not as good. Actually, I think that diversity is part of the strength. The question is, what is the partnership? All we are asking is that whether it is DHS or other entities within the government, that they are open and that they continue to build on the experience that we have been able to gain.

Ms. LOFGREN. Thank you, Mr. Chairman, for allowing me all that extra time.

Mr. THORNBERRY. I thank the gentlelady for some excellent questions.

Ms. VanDe Hei, let me ask you, you have heard and you are familiar with Mr. McCurdy's organization. Does the ISAC Council have a position on whether other cross-cutting organizations or information-sharing organizations are good and should be brought into the system in some formal way? What, if any, position does the ISAC Council have about that?

Ms. VANDE HEI. The ISAC Council, like I mentioned, wants to be inclusive, rather than exclusive, so we have gone from 8 to 14. Basically what it takes is for somebody from that particular information-sharing organization to come and talk to us about what they do. I am not aware of anyone being turned away.

Mr. THORNBERRY. But you do not have, that meets regularly with the ISAC Council do you, some sort of a cross, I am using cross-sector, but you know what I am trying to say, companies in different businesses that may share a concern over cyber security in this case. Nobody like that sits at the table with you, do they?

Ms. VANDE HEI. I guess I am not quite understanding the question, in that all the ISACs that sit around the table represent different sectors.

Mr. THORNBERRY. Right.

Ms. VANDE HEI. So I sit next to the electric sector, and water depends upon electric. And I sit next to the railroad people, and water depends on the railroad. So we have set up communications between each other so that when something happens like in the power outage, we were able to talk to the electric sector and to the transportation folks about how long the outage would continue. So maybe I am missing something.

Mr. THORNBERRY. I understand. ISACs are organized by sectors, and Mr. McCurdy's basic point is that maybe that is not the only way to organize; that you could have other organizations that cut across different kinds of businesses that could add an element to this debate. I do not want to give his arguments for him, but maybe you could even argue that if you are not strictly organized by sector, you would be more likely to share information because it is not your competitors that are setting right there with you. There are other pros and cons. I am just trying to figure out whether the ISAC Council has formally taken a position on these other kinds of organizations.

Then Mr. Dacey, I want to get to you and see whether you have analyzed these different ways of organizing ourselves. Part of what concerns me is we could be here 5 years from now and still be talking about different ways to organize ourselves, and we may not have really done anything. So in some respects, we have to do something even if it is imperfect just to move the ball a little bit.

Do you have anything else? Then I will go to him.

Ms. VanDe Hei. There is no barrier to a group like Mr. McCurdy's from joining the ISAC Council at all. You do need to be aware there is another group of sector coordinators that have met under the PCIS, Partners for Critical Infrastructure Security. That group is predominantly cyber-focused and brings together companies from all different, Cisco, you name it, they are part of this coordinating group. The ISAC Council meets with them regularly now as well, so that we are sure that the sectors are looking at the bigger picture; that the ISACs are in tune with what they are doing. So we have begun to meet jointly to ensure that. But just to answer your question, there is no barrier with an ISAC that does things differently from joining the ISAC Council and perhaps informing us about how better to do things. "Evolving" has been maybe overly used today, but we are looking for ways to do this better.

Mr. Thornberry. Yes, absolutely.

Mr. Dacey, what can you help us with here?

Mr. Dacey. I think, again not to be too trite about the"evolving," but I think things have changed a lot and there are continuing developments and very positive things have happened. When this first started in PDD–63 it in fact envisioned one ISAC for everybody, and then it was quickly determined that really a sector-based approach would be more appropriate at that time.

There are some benefits that we have identified in talking to a lot of people and working in this area for a while. First of all, there is a significant amount of industry-level expertise that exists that is very important for the analysis side of this whole equation. So I think you have to factor in how you get that sector-level, industry-level expertise for the various sectors; how some of these threats translate into impact.

I think also there are established and building trust relationships within those sectors, because people know each other. A lot of them are in associations where there is always some affinity and some aggregation of interests. So I think there is some benefit, too, there in terms of that trust relationship, which I think is very critical to this whole process. They are unique at this point in meeting the sector needs.

At the same time, the ISAC Council is a relatively recent event on the spectrum of timelines since we started this in1998. I think the opportunity exists for them to start sharing with each other and breaking down those silos. I think that is particularly important in an area that has not been talked about, but not extensively pursued. I know it is on everybody's radar screen, and that is interdependencies. That will drive the discussion of the need to work together and it will be in everyone's self-interest. I do not think we are quite there yet. I think we need to evolve to that point so everyone really understands how is my sector affected by that sector, so I care about what they are doing.

Second, the sharing and getting together can bring about a lot of good practices that are really out there and that can help others and benefit everyone across the community. It is fair to say that some of these ISACs have been more at the forefront than others. They have been around a long time. Some of them have a long-standing relationship with the Federal Government, which has been a step up for many of them.

So I think in answer to the question, you need to keep that industry-level expertise and trust relationship, and you need to figure out ways to start bringing them together collectively. I think that started at the ISAC level. It is starting at the sector coordinated level. I think that needs to be built up over time. The question is, how much time and who is in the best position to do that. I would leave it up to Ms. VanDe Hei just to talk a little bit about where they see it going, but that is my view personally on the way that needs to develop. It needs to be integrated in the end, so there is no silo.

Ms. VANDE HEI. Could I make one statement?

Mr. THORNBERRY. Sure.

Ms. VANDE HEI. It was the primary purpose for the ISAC Council to come together to talk about interdependencies and how we might work together, but this brings up another area where you could help us, in that I found in talking with the intelligence community, whether it was with the FBI or now with DHS, that they tend to be as stovepiped as we are or when looking at a threat. If it is a threat to electric, then it is an electric threat, and not necessarily a water threat or not somebody else's threat. So bringing together their analysts that look at the different sectors and having them look together in terms of the interdependencies and what the threats might be to them, I think is a fairly new phenomena. I am not sure it is taking place very well.

So I think as they begin to look at things in an interdependent way, that information will be coming to us in that way as well.

Mr. THORNBERRY. I think that is an excellent point. It is part of what raises these questions in my mind. For example, if you have an issue related to electricity, it goes, say, to the electricity ISAC and the people who regulate it are going to be focused on it. But what about all the customers of electricity? How can they prepare for some eventuality?

Cyber is another example which cuts across every sector, which makes it, I will not say unique, but I think has some particular characteristics. I suspect this is why Mr. McCurdy's organization is focused on cyber. I do not know how many others there are like that, telecommunications, electricity, cyber, probably cut across just about everybody. But some way, we have to consider not just the producer side, but the consumer side of these ISACs. I am not sure we are there yet.

Mr. McCurdy?

Mr. MCCURDY. Mr. Chairman, actually that is a great point. There is one interdependency now. There is one continuum, and that is we are hooked up to the network. The Internet has become that glue. So cyber is a cross-cutting modality that I think we need to be concerned about.

The other is, there has been a history with the regulated industries. Why is the FS–ISAC more mature? Because they have been in a regulated industry, or you look at some of the others. Part of our concern was, as I sat in PCIS and other meetings, oftentimes, and I know the industry well, most of our members in the association, you usually had security people in a room talking to security people about what the threats were, as opposed to engaging the consumer and the user. That is why we shifted our focus. I think that has been the maturation of the Internet Security Alliance. That is why we have companies like Coca–Cola. They are not dependent upon one factor or another. They are a user of the Internet.

Ms. VANDE HEI. Water.

Mr. MCCURDY. Water, OK. Yes, we are all dependent upon water. We are 98 percent water, right?

[Laughter.]

But the key is that there has to be, the Internet is the interdependency, but it is also the one area that is least regulated. So back to the question that Ms. Lofgren asked earlier, what is the way that you are able to engage the users in as deregulated a way as possible. I think that is the approach clearly that you have had working from your district in California in that industry, is you do not want to go to the old telecom model or to another model. You are trying to find a way to engage people in the Internet world. That is why we have to look at incentives. That is why your industry leaders are standing up every day saying here are some things that we ought to be looking at.

Mr. THORNBERRY. This is an interesting conversation. I do not want to continue on forever, but that does make me think to a critical point that Mr. Dacey includes in his report citing the ISAC Council that says the greatest barrier to information sharing stems from the practical and business considerations that although it is important, the benefits are kind of hard to get your hands around, but long-term it gets back to Ms. Lofgren's point that maybe the national interest. It is more amorphous and the rubber does not really hit the road until something happens, and that is part of our challenge, I think, in trying to sort our way through all this.

Mr. MCCURDY. We have actually looked at three areas, if I could, Mr. Chairman.

Mr. THORNBERRY. Sure.

Mr. MCCURDY. What is going to get the C-level interest? Sure, regulation will step up there and taxes would. But I think it is clear that they are interested from a marketing standpoint, and there are some market advantages. They are looking at a cost standpoint and potential liability. If we can help reduce their liability by becoming a qualified member, which is what we are trying to do, and this is where the maturation has occurred. You cannot be a qualified member if you do not have some way to measure that, and so you need some metrics. That is why we are working with the consortia on global security to develop metrics and tools so that we can actually have the benefits like insurance and reduced potential liability. So there are a number of these things that we are working on.

Mr. THORNBERRY. And those would be metrics set by some organization, not set by government regulation or law that would freeze them in place.

Mr. MCCURDY. That is exactly right.

Mr. THORNBERRY. OK.

Let me turn to slightly different issues, if I may. Ms. VanDe Hei, you were patiently here listening to a lot of questions go to the Department, Mr. Liscouski, earlier about vulnerability assessments and what they are doing. What is your overall view, or what is the overall view of the ISAC Council, if you can, about where the Department is, not just in giving out information that it has, but in receiving information from the various sectors.

Ms. VANDE HEI. I think the flow of information from the various ISACs is, I would not say it is limited, but it is different depending on the ISAC in question. I think that for some ISACs that are, my ISAC is made up primarily of publicly owned entities. Most drinking water and waste water systems are publicly owned. So the sharing of information with the government is not new to these people or with each other, because they do not compete with each other. So that is a fairly easygoing sort of sharing of information.

For some of the other sectors, it is proprietary information. Am I getting at your question?

Mr. THORNBERRY. Yes, yes.

Ms. VANDE HEI. It is more difficult to share with the government. Mr. Liscouski talked about the new CII program which is intended to provide the private sector with some place to put sensitive information or proprietary information and expect some confidentiality or protection to that information. I think the proof will be in the pudding on whether or not that program is sufficiently protective that it actually gets information from entities or the private sector that is concerned about that.

So I guess I cannot speak for all of the ISACs, but I suspect that the sharing of information is very different depending on whether you have competition, that you have trade secrets, that there are things you want protected.

Mr. THORNBERRY. It goes a little bit to the point made earlier that more regulated industries are in a different situation than less regulated industries.

Mr. Dacey, what is your perspective on how far along the Department is as far as getting and receiving information?

And second, do you think it is clear for an industry to whom they report information? It is not at all clear to me, for example, if the water industry says, well, we have talked and we think we may have a little problem here. Who do they go tell it to? Is the structure within the Department such that the answer to the second part of that question is clear?

Mr. DACEY. Two things, I think unquestionably there has been a lot of effort and actions being taken by the Department to try to address a lot of the issues that have been understood as being challenges going forward. Again, Mr. Liscouski elaborated on quite a number of those activities earlier today. I think things are improving. We are hearing about regular meetings taking place from both sides. With ISACs and the Department, there is more and more sharing of information.

I think the critical issues, though, get down to a couple of things that need to be done. We talk about that in our testimony. That is, I think the roles and responsibility of all the respective players deserves to be clarified a bit. I know we have this national infrastructure protection plan that is due out by the end of this calendar year. I realize it is being built up on a sector basis and it will be issued. I think it is going to be important that that lay out some of those roles and responsibilities, as well as initiatives, clear milestones, something that you all as Congress can look at in an oversight capacity and measure progress, some of the things that you need to see, well, when are we going to have this or that; is that the right strategic direction for the Department to take across these wide variety of areas we have all been discussing today.

At this point, we do not have that. We have had interaction and discussion with the Department, and they have shared with us their thoughts and ideas, but to a large extent we do not believe that is immortalized in writing so that somebody can independently look at it and understand and evaluate the process. Again, I do not want to insinuate that they are not doing things. It is just that we have not seen it documented in a way that it could be independently reviewed.

The other part of that is really coming up with the detailed procedures and policies. If you look at HSPD–7, that was one of the charges that the Department was supposed to develop those to help clarify, including the issues that you talked about. Who do you report to? In our discussions with the Department, they indicated that they were not going to try to make everyone go through one single point in the Department because they felt if that person was not available or could not get through, it would be problematic. Some of the cyber issues would seem to naturally go to the NCSD, which is the Cyber Security Division, and we know the ISACs have those issues. They indicated that they were developing processes or planned to develop process to coordinate within the Department the contact information as it comes in so that if it came in one place, the other people who needed to know would know. But I do not think that is in place today.

I do think there is some confusion from what have heard about who to talk to and who to report to. Again, as with anything, there are some trust relationships that are probably built up over time in certain parts of different organizations in the government that people would probably prefer to contact. We need to figure out a way to make that easier, and set up kind of a policies, procedures and clarity in what is the expectations are for that contact.

Mr. THORNBERRY. Mr. McCurdy, go ahead.

Mr. MCCURDY. Yes, just one quick point on cyber. Cyber, again, is a little different as far as sharing information. I have found even at the international level the one trusted organization that people are more willing to enter into discussions with regard to threats and vulnerabilities has been the CERT/CC. However, our concern is the timeliness of the information as they change the nature and move to the U.S. CERT. I think there is a concern that it will become too large and too bureaucratic. Right now, it works reasonably well because there is not only a trust relationship, but there are ongoing dialogue and conversations beyond just the threat warnings. It goes to what does it actually mean.

Eventually, we want to get out of the reactive mode into the prevention mode, where we can work with our industry and say, if you take these prophylactic steps, or if you do this, then you are better protected against potential threats or attacks regardless of the nature.

One last point on that, we have members that are members of ISACs, Financial Services ISAC, the IT ISAC, and they have become more involved with us primarily because of the value add on top of just information. It is the value add that is going to be to them the most important, when they have to go justify their cost to their bosses, and those value adds are again, the market-based incentives, the best practices, the public policy, just letting them know what is going on is critical, too.

Mr. THORNBERRY. Actually, you anticipated the question I was going to get to next, and that is, as U.S. CERT comes along, do some of your members have concerns that it is too much of a government agency in order to have that sort of trust relationship continue that they have had with the Carnegie Mellon CERT?

Mr. MCCURDY. It is interesting. The CERT/CC when it was originally Carnegie Mellon, was a hybrid. It was funded by government, but it was actually run by an academic institution. We in industry when we all saw this triangle, we had government, academic and industry, there was a lot of friction there and concern about how well they actually could work together. I think our experience has been over time that we have been able to overcome the worst things of academia and the worst parts of government mentality and probably some of the worst instincts in industry, to have a working relationship.

That is what I think our members are most concerned about is losing that synergy that has evolved. It is going to take some time. What we would like to hear from you all, what we are hoping to hear from Amit Yoran and Bob Liscouski and others is that first of all we are not going to break what is already working with a very successful organization, and that is access to the CERT data, just like the ISACs are going to have through the U.S. CERT. That is a baseline for us. Once we know that, then we are entering into additional relationships with Carnegie Mellon because they are creating what they call a CyLab to take it to another level of trying to add value.

What happens to U.S. CERT? We have all been involved with government. You have to conduct very close oversight, not on whether it meets timelines and all that, which is critical, but also what are the tendencies towards creating more and more bureaucracy, become more risk-averse, less open, less cooperative. Those are the concerns that we have as big institutions start to emerge. When that occurs, when it becomes a bureaucracy, watch industry go the other way. Then you are going to have to regulate to get them involved. Right now, it is not there, but if we are not careful, if we do not work with them, you could end up with that result.

Mr. THORNBERRY. The problem is, once you see that happening, it is too late.

Mr. McCURDY. Yes.

Mr. THORNBERRY. It is hard to reverse.

Mr. McCURDY. You are in a different situation. This is not the 1940's. This is a work in progress and the fact that you are having these having these hearings, there needs to be dialogue. I think your staff is having those dialogues. If a government entity learns anything from a hearing like this, and that is, they need to hear the questions and what is behind the questions. The questions are not always artfully phrased, but there is a genuine concern behind those.

Mr. THORNBERRY. Something is going on.

Mr. McCURDY. That something is going on. That is where this dialogue is critical.

Mr. THORNBERRY. That is right.

Ms. VanDe Hei, let me get back to you just to clarify. If the water folks got together and said, oh, we have this problem that we have not told anybody about. Would it be clear to you who in the Department of Homeland Security to go talk to about it?

Ms. VANDE HEI. No. Yes, and no, OK? They have a watch unit that you can call an 800 number and report an incident or a number of incidents to. I actually had experience with trying to do that. This is not particularly sensitive information, but there were seven to ten utilities in the Northeast that received threatening letters postmarked the same place. So I gave that information to DHS and to the WaterISAC analyst. I waited a couple of days and did not hear anything back. So I called. I was told that it had been dismissed; that they did not deem it to be credible, I guess. I asked on what basis and that sort of stuff.

But I am not confident at all, one, that I reached the right people, or two, that it was reviewed in a way that made sense. Two weeks later, I got a call from the police department in New York State that had not dismissed the letters. So no, it is still a maze and I think that there are a number of places where you can call and refer things, but I do not have a comfort level that I hit the right place or that it was reviewed. It might have been, it is just that that is a secret to me.

Mr. THORNBERRY. I think a lot of people have that concern, not just for immediate information that you have, but in trying to look at an industry and say, OK, what are some vulnerabilities; maybe we better talk to somebody about it. You never know. Do you go to the IA; to you go to the IP; how does all that work.

Ms. Lofgren?

Ms. LOFGREN. Just one final question. This has been very helpful. I know it is a long day to sit there, but it has been very helpful to me to hear what you have had to say. It is really for Mr. Dacey since you reviewed all of this. I will use water as an example, but I think it is equally true for any of the sectors.

You have people involved in, say, a water wholesaler in Santa Clara County, the water district. They know water more than they know terrorism. Unless they are reading Tom Clancy novels to figure out what could go wrong, they may see a vulnerability, but it may not be what the Department of Homeland Security might see. We know, taking water again, because of delusion, putting a substance in the Crystal Spring Reservoir is not something I am going to lose any sleep over because it is going to be diluted. It is not going to be effective. But what the Department of Homeland Security might, for example, see as a threat to water would be pollution, say, if you dumped some PCBs in Crystal Springs Reservoir. It would not really kill you, but it would disrupt the distribution of water in a way that is significant and serious and have a huge economic impact. The water wholesalers might not see that, but DHS might. Theoretically, they are doing a list of what we should be worried about. How is that list being assembled and how is it being communicated to the various sectors to guard against the Tom Clancy novel scenarios? Or is it?

Mr. DACEY. I cannot speak exactly to what they are doing in that regard. I can say from a standpoint of what direction I think needs to be taken and is being taken, is that even starting in 1998 the idea was that the sector coordinators and at that point lead sectors, now sector-specific agencies were to sit down and look at vulnerabilities on a sector basis, the kind of high-level vulnerabilities. What are the types of risks and threats? I think Mr. Liscouski talked about that earlier this morning. And assess them and determine how significant they are, again, not at an entity level, but at a sector level.

I am not familiar with how far they have gotten in that process. In theory, some of that will be addressed through these sector plans that are being part of this national infrastructure protection plan, but perhaps you might get more specifics on the water.

Ms. LOFGREN. I was just using that as an example.

Mr. DACEY. As to how the water sector is involved in that process, so you might be able to provide some information.

Ms. LOFGREN. You could have the same question about electricity or banking or Internet technology.

Mr. DACEY. Right. But that has been again on the books since PDD–63. We have had some initial strategies that came out from many of the sectors, but I do not think they have dug down to that level in detail about specific vulnerabilities and going through a formal assessment of the risks related to those.

Ms. VANDE HEI. For the water sector, in addition to the utilities doing a vulnerability assessment, EPA was required to do a threat document that was distributed to every water system that served over 3,300 people. So they tried to bring the two together so that people would have something to assess their vulnerabilities against. That kind of document, as far as I am aware of, has not come out of DHS, and the one from EPA was done a couple of years ago, and I think could use some improvement.

I think you would hear from DHS that providing threat guidance is one of the hardest things they have to do, because it is a moving thing, it is a moving target. What is the threat today to D.C. versus what is the threat someplace else tomorrow or the day after? I am not aware of any document like that that is available, but it is needed. It is desperately needed.

Ms. LOFGREN. All right. Thank you, Mr. Chairman.

Mr. THORNBERRY. Thank you.

I have just two or three final questions I would like to ask. Mr. McCurdy, there are lots of articles in the press today about a reported new vulnerability on the Internet. The Department had issued a warning about it on Tuesday. We are in the middle of something. How do you see where we are at being able to get information out and to do something to fix a vulnerability, now that we are kind of in the middle of one of these episodes?

Mr. MCCURDY. First of all, there have been four in the last couple of weeks. The one that was listed in the paper about TCP obviously got headlines because there is an announcement by a British citizen that I think is having a press conference or something. In most instances, the vulnerability is communicated prior to even the threat level. In some instances, we worked literally months with our trusted members, including the vendors, to address the vulnerability prior to it becoming released. That is this whole sensitivity of who actually gain access. That is why you do not make it all public.

Now, it is true sometimes we get something reported on CNN before we do CERT, but that is generally not the case. If you look at the numbers of vulnerabilities and threats that are being reported to the CERT, it has gone up exponentially every year. It is over 100,000 threats that are reported this year and probably 5,000 or 6,000 vulnerabilities. Vendors can go crazy with those things and there is this tension between the vendors and the users, and what is the appropriate reporting period and how do you assess this and how do you get them the opportunity to try to address it before it becomes public.

It is not just a question, as I said earlier, of just the threat reporting. It is true. It is out. What is really critical is how the reports are made. I have examples of those that we sent to our membership. It not only identifies the threat, and we do digests of lists of all the recent ones, and how you can go into a secure site in order to understand it better. But it talks about the vulnerability on the systems affected, the overview, the description of what it is, which sometimes is very lengthy and for many of us we could not understand a word it says; the impact. But more importantly, there is a solution. That is where you need the time and this trust relationship. The solutions often come from that communication with the industry.

When we are talking information sharing and people say it is proprietary and they do not want to release it, it is usually general counsel's that are kind of sending that message, the lawyers are out there saying that. But the people who work it every day, when they have this conference call that we have and they are saying, well, this is how we are dealing with it; boy, lights go on or this is how the experts at Carnegie Mellon or Southern Cal or Purdue are dealing with it. And then obviously they say apply a patch from your vendor. Well, that is an easy solution sometimes.

It is pulling all those people together that I think we have evolved to the point we now have that working. That is why some of our industry members are willing to pay so much for that. It is also why some of the other companies are sitting out there glad that they are paying that and are doing that because they are getting a free ride off of them. But then once you get that threat information, how do you develop the practices to ensure against it in the future and get out of the reactive mode.

Mr. THORNBERRY. Let me ask, to just get back to the central focus of this hearing, which you raised. Do any of you see a step that Congress needs to take to better protect, whether it is private sector data or whatever, related to critical infrastructure? Part of this, we are still feeling our way through. The protections we have already granted, is that enough? But at this stage in the proceedings, is there some additional step that you see that we need to take in order to help develop this trust relationship to share that information?

And if you do not, say no. I am just curious at this stage whether you do.

Mr. DACEY. Yes, just to step back a bit. A few years ago we reported on a lot of the concerns by the private sector with the FOIA and civil liability and antitrust being three of the primary areas of concern at that point. Certainly in the deliberations of Congress, you put provisions in the Homeland Security Act which provided certain protective measures forFOIA and those have embodied themselves in the CII process. Again, it is not a final rule that is in place. I think it will take a little time to figure out if that is adequate or not. So I do not know that I would rush to change that dynamic at this point until we see. Obviously, one of the issues gets back to risk. There has to be a benefit perceived in sharing that information as opposed to a potential downside that might exist. So I think that some of that will take time.

In terms of some of these other issues, I think, again I would go back to a comment that I made earlier that I think it is important that some of the strategies and some of these plans be laid out, and that be in full cooperation with the private sector and state and local governments. That is happening now and I hope it happens well, but it needs to be fully bought into by all those parties. As part of that process, I would hope they would be identifying along the way issues as you discussed, where legislative relief is appropriate or would benefit them. I think that would be the best process to follow.

If you get all these heads together, you are going to come up with a good list and then you can consider whether you want to deal with that collectively. At the top of my head, I do not have any just glaring issues that need to be addressed from a legislative standpoint, but that is certainly one area to think about going forward. Again, that is supposed to be out this fall, and it is going to be critical that all the players join in on that effort. I am hoping that that will happen.

Mr. MCCURDY. Without that final rule on FOIA, there is not the communication. The communication also has to be a two-way street. Mr. Liscouski used the magic words, probably because that is what we are preaching to them. Do not expect just to have private industry tell you all the vulnerabilities, and then have it go off into some massive organization never to get reported back or some affirmation that it was useful or not. If it is just that flow, then it will be cut off. That information will not flow.

The other thing just from being on both sides of these tables, I think effective oversight is a neglected art and I think you are doing it here. Do not just think you have to have a bill. It is always fun to have our names on legislation, but I think following up regularly and, you do not have to beat them up, but it has to be a communication, and it too has to be two-way. They need to be sensitive to that.

It certainly would help if this committee becomes a permanent committee that the different lanes of jurisdiction are addressed, because I feel for these individuals in government who spend all their time trying to deal with stakeholders. They are hearing from us in the private sector, but they are hearing from you as the overseers, as the board in effect, and they cannot do it all. I do not care how big the staff is. The more staff that they have, the more staff that you will have, the more requests that get going back and forth.

So I think there has to be some good on-record conversations and there probably has to be some good off-the-record field discussions that take place. I always found those to be the most interesting and informative. We would invite you, by the way, there are facilities nearby. I know you have seen a number of those, but in the cyber world that are quite remarkable. Seventy percent of the world's Internet flows just a few miles from here. Some of our members, where it is a VeriSign or at the very hub or the old Cable and Wireless, which is now another company, but they control a lot of the critical nodes. They are the pulse of a lot of activity that is pretty amazing. It takes a very professional set of wisdom and experience in order to understand what that all means as it goes through. Government is not going to do that. That is in the private sector.

So I would encourage you to do what you are doing. I would encourage you to reach out to industry more because industry does not understand always your drive from a national security perspective. They are market-driven, but the market can work in favor of national security if we have the right kind of exchange, and we would welcome that.

Mr. THORNBERRY. Thank you.

Ms. VanDe Hei?

Ms. VANDE HEI. I guess I would suggest that perhaps the bioterrorism bill that was passed in June 2002 had some protections in it for the vulnerability assessments that needed to be submitted to EPA that were stronger than in the homeland security bill. In fact, there were criminal penalties attached to misuse of the information. I think that you might want to tighten up that part of the legislation to add to the comfort level of some of the private sector. It certainly did give some comfort to the drinking water systems because they do feel fairly vulnerable.

The other thing I would like to add, though, to Mr. McCurdy, is that your oversight of the Department, I think it is very important that Homeland Security needs to be done differently than any of the other departments and how they work. We are regulated by EPA and we know how that works and what the thought process is. But security cannot, I think, succeed in the same sort of bureaucratic stovepipe kind of thinking. What I see as the Department grows, when somebody says to me, hi, I am so and so and I have been in the government for 30 years, my comfort level does not go up that it is going to be done differently. So I think it is really important that you keep an eye on keeping it lean and mean and that they are doing things in a way that is different, so that regulation is not the only answer that you see down the road. I think that can be done and I think it is important that we try to do that before going in any other direction.

Mr. THORNBERRY. I appreciate all three of you and your valuable insights. It has been very helpful for me. I appreciate your willingness to be before us. I also appreciate your willingness to answer some written questions if there are follow-up things that we need to submit.

With that, this hearing stands adjourned.

[Whereupon, at 2:34 p.m., the subcommittees adjourned.]